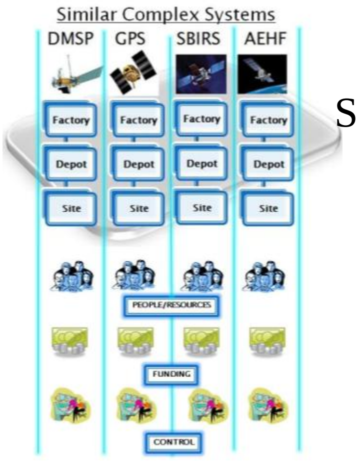
Integrated Maintenance System

Integrated Maintenance Mission Operations Center System Study

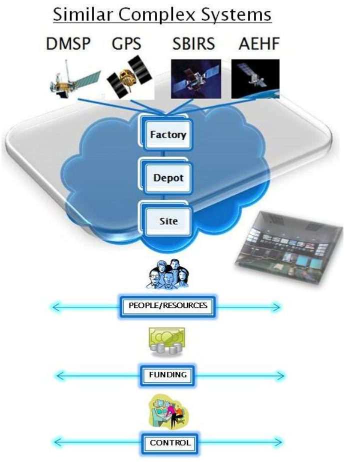
Dr. Kathryn Laskey, Advisor
OR 680, Spring 2007
George Mason University

David Dumont, Sponsor
Senior Program Manager: Operations and Systems Evolution Support
Mission and Combat Support Systems
Information Systems & Global Services
Lockheed Martin Corporation

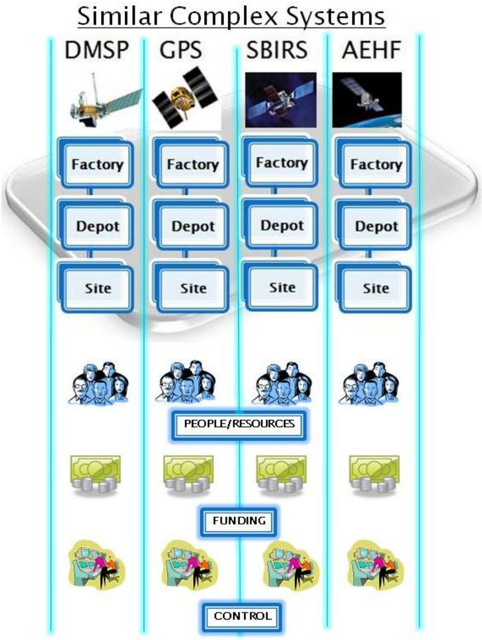


By:
Joshua Icore – G00446651
Mark Icore – G00446653
Scott Sweeney – G00429135

Thursday, 03 May, 2007

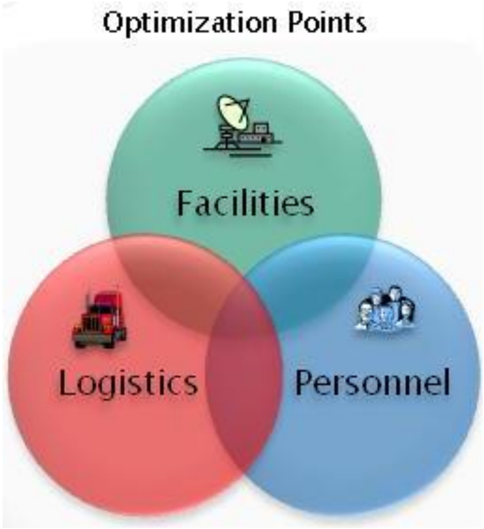


Executive Summary

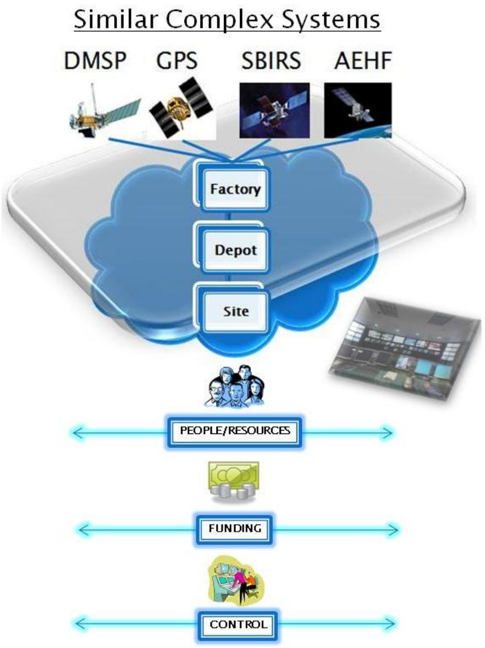


Historically, space-based systems such as those procured and operated under the auspices of the United States Air Force Space Command and United States Strategic Command each contain a dedicated maintenance segment focused on maintaining the operational state of each of the various mission segments. The organic maintenance segment provides the complete set of physical and logical maintenance functions from hardware replacement to software upgrades and includes a complete set of maintenance facilities (depots and factories) as well as the personnel to execute the maintenance tasks and a logistics system to move people, parts, and data between operational and maintenance nodes.

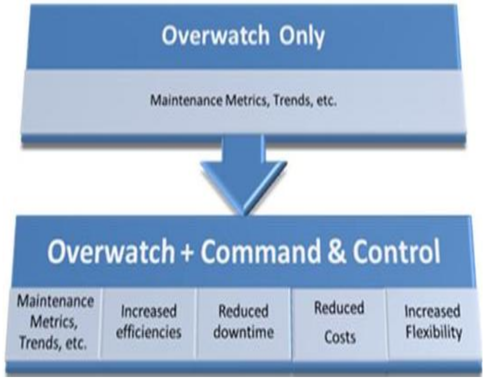
The vertically integrated maintenance segments provide operational system commanders with a high degree of confidence that the maintenance segment will sustain the mission of the operational system. However, the confidence comes at a cost – the maintenance segment is often specified to meet “worst case” scenarios rather than likely case scenarios. Worst-case scenarios are often defined as critical failures in multiple independent subsystems of the mission system. While it may be necessary, in rare instances, to execute maintenance on multiple subsystems to return the system rapidly to an operational state, the result of the worst-case specification is the creation of a standing army of people staffing multiple facilities geographically dispersed to survive whatever disaster was the basis for the worst-case scenario.



While robust, the creation of an organic, vertically integrated maintenance segments for each operational system is not cost effective. Cost effectiveness of organic or dedicated maintenance segments decreases due to excess capacity within the maintenance segments because of a need to scope each maintenance segment to the worst-case maintenance scenario for that operational system. Cost effectiveness is further reduced when the commonality of hardware and software components across the various space systems is considered. Commonality of components indicates that each organic, vertically integrated maintenance segment invests in duplicative capabilities. Further, many of the maintenance actions are performed by contractors, many of which work on multiple operational systems providing similar or identical maintenance actions on each of the operational systems.



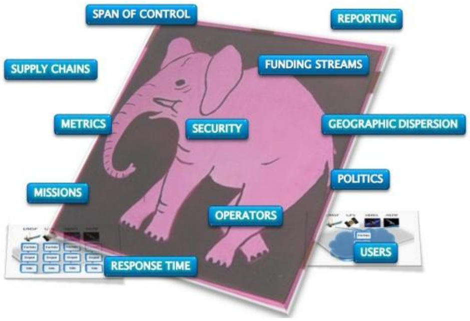
As evidenced by the extensive debate surrounding the funding of the war in Iraq, the national security imperatives of today do not guarantee or protect defense and intelligence budgets from public debate and questions of return on investment and cost effectiveness. This is in direct contrast to the last fifty years of the 20th century – the time during which many of the existing operational systems and their vertically integrated, organic maintenance segments were acquired and built. Therefore, given the increased scrutiny on budget expenditures and systems acquisition[1], current constraints on budget due to military operations in Afghanistan and Iraq, as well as other new system acquisitions, it is necessary to investigate the feasibility and practicality of consolidating the various space-based maintenance segments into an integrated maintenance system supporting multiple mission systems.


Overwatch Only
Maintenance Metrics, Trends, etc.
Overwatch + Command & Control
Maintenance Metrics, Trends, etc.
Increased efficiencies
Reduced downtime
Reduced Costs
Increased Flexibility

The integrated maintenance system, executing the maintenance mission, has two primary missions aside from actual execution of the maintenance tasks. The first mission is Overwatch, or collection and display of maintenance of status of the entire system. Overwatch enables a central organization – the Integrated Maintenance Mission Operations Center – to monitor the status of resources and maintenance tasks throughout the maintenance system, enabling capacity planning and the leveraging of economies of scale through consolidating communications, equipment, facilities, logistics, and personnel resources.

The second mission is Command and Control, or the direction of maintenance actions throughout the integrated maintenance system. Command and Control enables the Integrated Maintenance Mission Operations Center to direct actively the execution of the maintenance mission. The active direction of maintenance tasks enables all of the resources of the entire maintenance system to be used in supporting each of the operational systems rather than the default

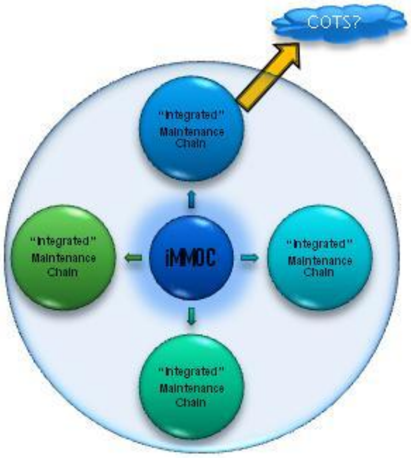
[1] Examples of systems cancelled due to system acquisition pressures include the Navy A-12, the Army Areal Common Sensor, the Army Crusader howitzer, the Army Comanche helicopter. Delayed systems, or systems with reduced production include the F-22, F-35, and the Air Force Tanker revitalization program.



fraction of resources allocated to a given operational system. Therefore, using the Command and Control mission, the entire maintenance system can be sized to one or more worst-case scenarios, but the resources acquired specifically for worst-case rather than most-likely-case scenarios are available to all operational systems, reducing the waste and excess capacity within the integrated maintenance system.

Using a combination of techniques oriented towards mission analysis of an integrated maintenance system, including interviews with subject matter experts, structured design, requirements elicitation and decomposition, and functional decomposition, the team prepared a framework and common language for the next stage of analysis in examining the cost feasibility of the integrated maintenance system.

This study identified the various stakeholders and obstacles – financial, operational, and political – as well as the numerous constraints – data, financial, legal, operational, personnel, security, and technical – and high-level requirements that influence the creation of an integrated maintenance mission and a supporting integrated maintenance system. Of specific note within this study is the identification of the significant negative impact that commercial- and government-provided hardware and software can have on the successful execution of maintenance actions and how that impact is hidden today within the organic maintenance segments. This explicit identification of the negative impact on maintenance execution of commercial- and government-provided hardware and software challenges the traditional assumption that off the shelf components are cheaper across the entire lifecycle than are custom-developed parts. When sustain activities are factored into the lifecycle, which often extend many orders of magnitude in time and cost beyond development activities, custom-developed components may be cheaper than off the shelf components.


COTS?
"Integrated" Maintenance Chain
"Integrated" Maintenance Chain
iMMOC
"Integrated" Maintenance Chain
"Integrated" Maintenance Chain

While facing significant challenges, many political, the creation of an integrated maintenance system to sustain operational space-based systems shows significant promise for cost and labor reductions. Further, there are indications that the integrated maintenance system can achieve an overall improvement in the execution of the maintenance mission across all operational systems as compared to the organic maintenance segments through the application of industry best practices such as the Information Technology Infrastructure Library (ITIL) and Capability Maturity Model – Integrate (CMMI).

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Illustrations

Table of Illustrations

Acronyms and Glossary

Acronym/Term	Expansion/Definition
$A(\infty)$	Steady State Availability (operational metric)
$\overline{A(t)}$	Mean Availability (operational metric)
A_a	Achieved Availability (operational metric)
A_i	Inherent Availability (operational metric)
A_o	Operational Availability (operational metric)
A_t	Instantaneous Availability (operational metric)
ACL	Access Control List
AD	Active Directory
ADPE	Automated Data Processing Equipment
AEHF	Advanced Extremely High Frequency (satellite communications system)
AF	(United States) Air Force
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFNOSC	Air Force Network Operations Security Center
AFOI	Air Force Operating Instruction
AFOSI	Air Force office of Special Investigations
AFPD	Air Force Policy Directive
AFSN	Air Force Systems Network
AFSPC	(United States) Air Force Space Command
ANG	Air National Guard
C&A	Certification and Accreditation
C2	Command and Control
C4	Command, Control, Communications, and Computers
CDB	Capacity Database
CDRL	Contract Data Requirements List
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CITS	Combat Information Transport System
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLS	Contractor Logistics Service
CMDB	Configuration Management Database

Acronyms and Glossary

Acronym/Term	Expansion/Definition
CMMI	Capability Maturity Model, Integrated
CONOP	Concept of Operations
COTS	Commercial Off The Shelf (technology/product)
D_0	Operational Dependability (operational metric)
DAA	Designated Approving Authority
DB	Database
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMSP	Defense Meteorological Support Program
DNS	Domain Name Service
DoD	Department of Defense
DODD	Department of Defense Directive
DSP	Defense Support Program (early warning satellite system)
EC	Equipment Custodian
ETM	Enterprise Telephony Management
FCAPS	Fault, Configuration, Accounting, Performance, and Security
GIG	Global Information Grid
GMU	George Mason University
GNO	Global Network Operations
GNOSC	Global Network Operations Security Center
GOTS	Government Off The Shelf (technology/product)
GPS	Global Positioning System (satellite system)
IA	Information Assurance
IDEF	Integrated Definition
IDM	Information Dissemination Management
IDS	Intrusion Detection System
IMMOC	Integrated Maintenance Mission Operations Center
INFOCON	Information Operations Condition
INFOSEC	Information Security
IP	Internet Protocol
IPS	Intrusion Prevention System

Acronyms and Glossary

Acronym/Term	Expansion/Definition
IS&GS	Information Systems and Global Services (LM business area)
IS&S	Integrated Systems and Solutions (Former LM business area, now part of IS&GS)
ISO	International Standards Organization
ISSO	Information Systems Security Officers
IT	Information Technology
ITE	Information Technology and Engineering (School of, at GMU)
ITIL	Information Technology Infrastructure Library
JCIDS	Joint Capabilities Integration and Development System
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
LED	Light Emitting Diode
LM	Lockheed Martin
LRU	Line Replaceable Unit
M&CSS	Military and Combat Support System (LM division within IS&GS, formerly IS&S)
MAJCOM	Major Command
MCR	Mission Capable Rate (operational metric)
MDT	Mean Down Time (operational metric)
MILSTAR	Military Strategic and Tactical Relay (satellite communications system)
MOA	Memorandum of Agreement
MOB	Main Operating Bases
MOC	Mission Operations Center
MOU	Memorandum of Understanding
MS	Microsoft
MSC	Major Subordinate Command
MTBF	Mean Time Between Failures (operational metric)
MTBM	Mean Time Between Maintenance (operational metric)
MTBSI	Mean Time Between Service Incidents (operational metric)
MTCBF	Mean Time Between Critical Failure (operational metric)
MTTF	Mean Time To Failure (operational metric)
MTTR	Mean Time To Repair (operational metric)
MTTRF	Mean Time To Restore Functionality (operational metric)
NATO	North Atlantic Treaty Organization
NBM	Network Battle Management

Acronyms and Glossary

Acronym/Term	Expansion/Definition
NCC	Network Command Center
ND	Network Defense
NETA	Network Attack
NETCOP	Network Common Operating Picture
NETD	Network Defense
NETOPS	Network Operations
NIPRNET	Non-classified IP Routing Network
NM	Network Management
NOC	Network Operations Center
NOSC	Network Operations Security Center
NOTAM	Notice to Airmen
NS	Name Server
NSS	National Space Security
NTP	Network Time Protocol
OI	Operating Instruction
OPREP	Operational event/incident report
OR	Operations Research
PCS	Permanent Change of Station
PDF	Portable Document Format
PERT	Program Evaluation and Review Technique
PMO	Program Management Office
POC	Point of Contact
RAC	Remote Access Client
RAS	Remote Access Server
RCM	Resource Capacity Management
S&NM	Systems and Network Management
SAF	Secretary of the Air Force
SAF/XC	Secretary of the Air Force/War Fighting Integration and CIO
SBIRS	Space-Based Infrared System (early warning satellite system)
SC2	Space Command and Control (Business unit within M&CSS division of LM IS&GS)
SE	Systems Engineering
SEOR	Systems Engineering and Operations Research (Department within ITE)
SIPRNET	SECRET IP Routing Network

Acronyms and Glossary

Acronym/Term	Expansion/Definition
SITREP	Situation Report
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
STRATCOM	(United States) Strategic Command
TACIP	Tactical Internet Protocol
TCNO	Time Compliance Network Order
TMAP	Telecommunications Monitoring and Assessment Program
TO	Technical Order
TSAT	Transformational Communications Satellite (satellite communications system)
USAF	United States Air Force
USG	United States Government
USSPACECOM	United States Space Command (DoD Combatant Command replaced by STRATCOM)
VPN	Virtual Private Network
XML	Extensible Markup Language

1.0 Introduction

This section introduces the Integrated Maintenance Mission Operations Center Study executed on behalf of Lockheed Martin Information Systems and Global Services Mission and Combat Support Systems as part of each authors' graduate degree program in systems engineering for George Mason University under the guidance of Dr. Laskey.

1.1 Background

Throughout the course of its history, space-based systems owned by the United States Government (USG), operated by the United States Air Force (USAF) Space Command (AFSPC), under the Command and Control (C2) of the United States (US) Strategic Command (STRATCOM) (formerly US Space Command [USSPACECOM]), have required a diverse set of maintenance depots performing software development, software maintenance, hardware maintenance, training, and logistics (e.g., licensing agreements, maintenance agreements, purchasing equipment, and inventory). Several examples of the many space-based systems in operation or development by the AFSPC and STRATCOM are:

- Defense Meteorological Support Program (DMSP) system, which provides advanced weather information to military planners
- Global Positioning System (GPS), which provides precision time and location information to users worldwide
- Transformational Communications Satellite (TSAT), Advanced Extremely High Frequency (AEHF) system and its predecessor system, the Military Strategic and Tactical Relay (MILSTAR) system, which provide robust, secure, jam-resistant military Command and Control (C2) communications to US and allied forces around the globe
- Space-Based Infrared System (SBIRS) and its predecessor system, the Defense Support Program (DSP), which provide early warning of a strategic missile launch

All of these systems (AEHF, GPS, DMSP, DSP, MILSTAR, SBIRS, and TSAT) have ground elements forward deployed around the globe. Further, since these systems support strategic missions (Command and Control of nuclear and strategic forces, early launch warning, military campaign planning), each system has multiple stakeholders across the USG, the North Atlantic Treaty Organization (NATO), and other governments allied with the USG.

Since the operational sites for these systems are globally deployed, so too are the depots geographically dispersed, providing support to multiple stakeholders, and receiving funding from multiple sources. Therefore, each systems will have multiple stakeholders around the globe and throughout the USG, with users of the system and military platforms having a stake in the operation and maintenance as well as functionality of the systems.

The continued deployment of AEHF, DMSP, DSP, MILSTAR, SBIRS, TSAT, and other space-based system payloads and ground station command and control and exploitation systems has occurred in temporal proximity to the growth in Information Technology (IT) capabilities and an increased awareness by the SBIRS primary stakeholder, the United States Air Force (USAF) Space Command of the value added by integrated logistics. Integrated logistics is a concept in which the entire logistics tail, including the maintenance activities associated with a deployed system are explicitly analyzed, modeled, and integrated into the maintenance and logistics activities associated with other systems, thereby preventing duplication of effort and reducing costs associated with maintenance and other logistics activities. Further, logistics activities are included in the operational aspects of the primary mission, raising activities traditionally viewed as non-value add, such as maintenance and spare parts management to their appropriate mission-support levels.

Fundamentally, integrated logistics requires the ability to treat logistics as a mission, just as strategic warning is the mission of SBIRS and secure, available strategic communications that of AEHF, MILSTAR, and TSAT, and high-precision global positioning and time that of GPS. Further, just as the AEHF, GPS, MILSTAR and SBIRS operations centers track the status of the various AEHF, GPS, MILSTAR and SBIRS segments – payload, spacecraft, communications, ground systems, and exploitation systems – to report on the mission status of AEHF, GPS, MILSTAR and SBIRS, so too must integrated logistics have a command center that tracks the various segments that make up the logistics tail of the system.

Today, logistics is performed on an ad hoc basis, with each system stakeholder responsible for certain logistics efforts and the various system Program Management Offices (PMO) responsible for others. To ensure mission effectiveness, each stakeholder invests in the maintenance activities they view as the greatest value add to their particular circumstances without regard for the system as a whole, leading to duplicate investment and underfunding of critical activities.

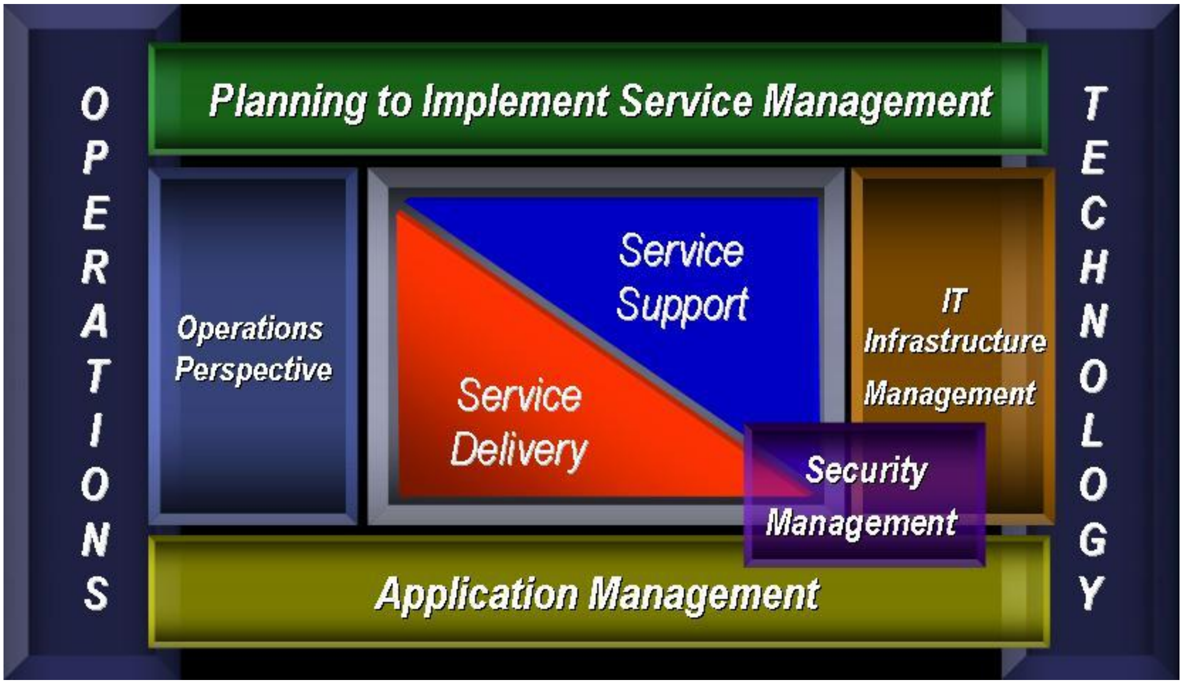


Figure 1.1-1: Interrelation Of Standards Models for Operations and Maintenance

As AEHF, GPS III, SBIRS, and TSAT transition into a fully operational capability over the next few years, there will be no new development money to fix issues that may be present in the system. Therefore, it is necessary to leverage the maintenance dollars provided by each stakeholder to ensure the optimal efficiency of the AEHF, GPS, SBIRS, and TSAT missions. To do this, one of the AFSPC and STRATCOM contractors is investigating the creation of an Integrated Maintenance Mission Operations Center (IMMOC) that will track the operational status of the maintenance mission, performing system Overwatch across the maintenance functions and possibly executing Command and Control of maintenance functions.

The IMMOC Concept of Operations (CONOP), authored by the project sponsor, is based upon service management, service support and service delivery best practice functions as outlined in the Information Technology Infrastructure Library (ITIL). Roles, Functions, Processes and Procedures are defined to conform with the International Standards Organization (ISO) IT Service Management standard (ISO 20000) and the Information Security Management standard (ISO 17779). Figure 1.1-1 provides a graphical representation of how various standards models apply to the integrated maintenance mission.

1.2 Desired Outcome

The sponsor desires to investigate physical and virtual consolidation of depots and factories to realize increased efficiencies, reduced system downtime, and reduced costs associated with maintaining spaced-based maintenance systems while providing assurances to stakeholders that such a consolidation will not result in degraded system performance.

1.3 Potential Study Objectives

In discussing the problems inherent in creating an integrated maintenance system for space-based systems, it became apparent that the study performed could accomplish numerous goals. Table 1.3-1 shows some of the study objectives that were discussed between the project team and the project sponsor.

Table 1.3-1: Potential Study Objectives

Objective	Constraints	Products
Propose an architecture that supports the CONOP objectives.	• Different government organizations are customers for each of the 15 programs • Separate funding sources for each program • Specific direction for funding usage on each program (colors of money for development, O&M, facilities, etc.) • Separate program schedules • Classification limitations • Organizational conflicts of interest • Export control • Global dispersed locations • Time zone deltas • Commercial vendor property control • Government vendor property control • Maintenance agreements • Licensing agreements • Multiple Bills of Material • Separate supply chain	Architecture Views

Table 1.3-1: Potential Study Objectives

Objective	Constraints	Products
Propose the organizational structure that will support the architecture	• Provide justification for how it supports the architecture and why it was selected. • Options can be provided as well with justification for those. • Provide options in preferred order.	High-level org chart for 1 organization managing the 15 programs, positions required at the program level and recommendation for what tier in the program level organization they need to fall.
Detail roles and responsibilities for top-level organization and positions at the program level.	• Research where this objective or related objectives have been executed in the past • Government or Commercial implementation	Product: Whitepaper detailing research efforts, quantitative data supporting or arguing against the objective, process guidelines used for implementation in those cases. Conclusion about why/why not it was good to do this substantiated with areas that were impacted positively or negatively for the customers.
Define the metric and measures of success for the organization		Quantitative Metrics Plan
Gap analysis between CMMI 5 for services and ITIL	To be provided to from sponsor: notional details of programs to include: name, value, capabilities provided to customer	Gap analysis, recommendation for which process to implement into this organization, and a tool for mapping programs into the quality model.
Quality model implementation plan		Plan to include, schedule impacts, performance impacts/improvements, and deployment schedule

1.4 Study Scope

In cooperation with the project sponsor, the George Mason University (GMU) student team negotiated a set of study objectives that met sponsor goals and GMU requirements for the project. This section outlines those objectives and the associated deliverables.

The study explores the integration of maintenance missions currently organized as vertical stovepipes within their operational systems. The AS IS state consists of maintenance and logistics segments wholly owned and operated by the system which they support. The TO BE state consists of a single, integrated maintenance system whose mission is execution of maintenance for all operational systems.

The study analyzes integrated maintenance through the lens of an Integrated Maintenance Operations Center (IMMOC), similar to Network Operation Centers (NOC) worldwide, within the IMMOC. The IMMOC provides a progressive drill-down view of the maintenance and logistics segments associated with AFSPC and STRATCOM systems. The IMMOC is the primary data repository and analysis center for decision makers responsible for the execution of the IMMOC and integrated logistics missions.

1.4.1 Study Objective

1. Define what it means to be an integrated maintenance system

2. Analyze the mission of the integrated maintenance system
3. Identify the parameters that the IMMOC will require in order to make maintenance mission readiness and operational capability assessments.
4. Identify benefits that can be obtained by the IMMOC if the IMMOC has a Command and Control role in addition to the "Overwatch" role defined by goals 1-3.
5. Define the Command and Control mission and parameters of the IMMOC required to make maintenance mission command decisions.

1.4.2 Secondary Goals

1. Identify components that need to be tracked and monitored by the IMMOC in order to execute the integrated maintenance mission.
2. Define what it means for the maintenance and logistics system to be "up" or "down" and to be "fully-," "partially-," or "non-" mission capable. These terms are well understood in the mission operations centers, but not in the domain of support centers.

1.5 Document Overview

This document is organized into front matter, an Executive Summary, 7 major sections and 5 appendices.

The front matter consists of the Table of Contents, the Table of Illustrations, and the Acronyms and glossary for the document.

The Executive Summary provides a synopsis of the entire study, including goals and objectives, analysis, and conclusions.

Section 1.0, *Introduction*, provides a high-level overview of the document. In addition to the document overview, this section identifies the project background, the desired system outcome, potential study objectives, study scope, key definitions, study resources, and roles and responsibilities of the study team, project sponsor, and project advisor.

Section 2.0, *Referenced Documents*, identifies documents referenced within this document.

Section 3.0, *IMMOC Study*, provides an overview of the team approach to executing the IMMOC study, assumptions made in execution the study, and open issues.

Section 4.0, *Integrated Maintenance* Mission , presents requirements for each of the IMMOC missions that must be satisfied for the IMMOC to execute its two missions. Additionally, metrics that should be measured as part of the mission execution are identified in this section.

Section 5.0, *IMMOC Mission*, defines the two primary missions of the IMMOC, Overwatch, or system monitoring, and Command and Control, or system direction.

Section 6.0, *Analysis*, presents pictorial representations of the physical, logical, and functional architecture of the IMMOC and relevant portions of the integrated maintenance system architecture.

Section 7.0, *Conclusions*, describes the key conclusions of the report and study including the challenge to the traditional presumption of the lifecycle cost effectiveness of Commercial Off-The Shelf (COTS) hardware and software over custom-developed hardware and software.

Appendix A, *Glossary Key System and Study Definitions*, contains definitions for key terms used in the study and forms the common vocabulary used throughout the study.

Appendix B, *Key Operational Metrics*, identifies key metrics typically associated with operational system and the definitions of those metrics.

Appendix C, *Industry Best Practices in Metric Selection and Collection*, identifies key considerations that Gartner and Burton Group make with regard to the identification and collection of metrics in operations and maintenance environments.

Appendix D, *Metrics Mapped to Operational Balanced Score Card Quadrants*, maps industry standard metrics to a balanced score card to assist in achieving operational objectives.

Appendix E, *IMMOC Objectives and Requirements*, highlights the objectives of the IMMOC and the integrated maintenance mission as excerpted from the requirements document assembled as a prelude to this study.

Appendix F, *Project Management*, contains supporting project management detail, including summary schedules and other related information.

2.0 Referenced Documents

Air Force Instruction (AFI) 63-101, Operations of the Capabilities Based Acquisition System

AFI 10-202, Operations Maintenance Scheduling

AFI 10-206, Operational Reporting

AFI 10-601, Capabilities Based Requirements Development

AFI 21-117, Core Automated Maintenance Systems Procedures

AFI 33-114, Software Management

AFI 33-115, Volume 1, Communications and Information, Network Operations (NETOPS), dated 24 May 2006

AFI 33-138, Enterprise Network Operations Notification, and Tracking

AFI 33-202, Volume 1, Intrusion Detection System Response Procedures

AFI 33-207, Computer Security Assistance Program

AFI 33-219, Telecommunications Monitoring and Assessment Program (TMAP)

AFI 99-103, Test and Evaluation Process

AFPD 37-1, Information Management

AFMAN 37-123, Management of Records

Allied Communications Publication (ACP) 121/United States Supplement (US SUP)-1, Communication Instructions General

Burton Group: Architectural Overview of Network Management, Version: 1.0, Oct 17, 2005

Burton Group: The IT Infrastructure Library: A Service Perspective, September 15/16, 2005

Burton Group: ITIL: Supporting the Service Chain Version: 2.0, Dec 05, 2005

CJCSI 3170.01D, Joint Capabilities Integration and Development System

CJCSM 3170.01A, Operations of the Joint Capabilities Integration and Development System

Concept of Operations, Maintenance Mission Operations Center, dated 7 March 2006.

DoDD 5000.1, Defense Acquisition Guidebook

DoDD 5000.2, Defense Acquisition Guidebook

Executive Order 12958, as amended by Executive Order 13292, dated 25 March 2003.

GMU Department of Systems Engineering (SE) and Operations Research (OR) (SEOR) Course Overview for OR 680, Applications Seminar, Spring 2007, Course Overview, downloaded 5 February 2007.

IMMOC SRD v5, Dated 18 March 2007

NSS Acquisition Policy 03-01

US Army Field Manual 3-0, Operations, dated June 2001.

Wikipedia online encyclopedia, http://en.wikipedia.org

3.0 IMMOC Study

The IMMOC study was conducted as an exercise in mission analysis whose purpose is to investigate what integrated maintenance means and to guide the execution of future work designed to investigate the feasibility of executing the integrated maintenance mission across cost, technical, and political domains. The study does not directly address any modeling of cost or performance, but rather focuses on identifying driving parameters and issues for future study.

3.1 Study Approach

The team applied numerous techniques to enable the successful completion of the study goals. Specifically, the team engaged in seven tasks, identified below, and applied them to each of the CDRLS identified in Section F.2:

1. Academic research – examination of literature relevant to the IMMOC CONOP and mission
2. Sponsor feedback – discussions and interviews with the project sponsor to ensure understanding and validate hypothesis
3. Structured decomposition – decomposition of the IMMOC into hierarchies of related components, including functions, physical elements, and missions
4. Requirements decomposition – documentation of IMMOC-specific requirements based on the sponsor-provided CONOP.
5. Mathematical models – where appropriate, identification of appropriate models that are useful to the understanding of the IMMOC and maintenance mission environment
6. Logical models – where appropriate, construction of logical models, including data models, system activity models, and entity-relation diagrams to assist in the understanding of the IMMOC and maintenance mission environment.
7. Project management – application of project management techniques, including Gantt and PERT charts to determine feasibility of completing the study tasks.

3.2 Top-Down and Bottom-Up Assessments

The two natural perspectives from which to view the IMMOC and the integrated maintenance mission – a top-down approach and a bottom-up approach. Both the top-down and bottom-up approaches viewed the maintenance mission as a hierarchy with the IMMOC as the root of the tree and maintenance depots as nodes and leaves.

The bottom-up approach started with the maintenance sites – the known entities – and attempted to identify those attributes of the site that were relevant to the IMMOC and the execution of the maintenance site mission. The top-down approach identified those attributes in which the IMMOC has interest and which flow down to the maintenance sites for fulfillment.

Table 3.2-1 highlights some of the basic differences between the top-down and bottom-up approach for analyzing and designing the maintenance mission and IMMOC.

Table 3.2-1: IMMOC-Centered vs. Operational Centered Design Comparison

Attribute	IMMOC Execution View	Operational Site View
Root Node	Factory	Operational Site
Maintenance Execution System View	Tree, with the factory as the root	Chain, with the site as the root
IMMOC Overwatch System View	Graph, with the IMMOC as the root and all nodes reporting to the IMMOC	Graph, with the IMMOC as the root and all nodes reporting to the IMMOC
IMMOC Command and Control System View	Forest composed of directed trees, with the IMMOC at the root and command paths flowing to factories, then to depots, and finally to operational sites	Forest composed of directed trees, with the IMMOC at the root and command paths flowing to sites, then to depots, and finally to factories
Maintenance Capability per Node	Union of capabilities of each parent node with the current node capabilities	Capability of each node
Maintenance Routing	Hidden from system Performed in concert with maintenance escalation in which each node passes tasks to its parent for fulfillment if it is not able to do so locally	System “source routes” maintenance requests, explicitly identifying which node performs which task
Detailed Maintenance Knowledge	Each node has knowledge of the tasks it executes and that its parent node can execute other tasks	The end system has detailed knowledge of each task and the order in which it is to be executed
Resource Optimization	Optimization capable of being executed by any node for the sub-tree of which it is the root	Optimization is possible only from each leaf node to the system root
Scheduling	Scheduling can be performed at each node for the sub-tree of which it is the root	Scheduling is performed by each leaf node for the nodes between it and the root.

3.3 Study Assumptions

Numerous assumptions were made within the confines of the study to enable achievement of the project goals. Assumptions were made to resolve unknowns or to simplify details that are irrelevant to the scope of the project.

3.3.1 Authorization to Co-mingle Funding

This study assumes that the IMMOC is authorized to comingle all maintenance funds received from operational systems for the execution of the mission. While this may not hold true in reality, the focus of the study is on the mission execution not the intricacies of funding authorizations and appropriations.

3.3.2 Scalability

The study assumes that the system has infinite scalability. While scalability comes at a cost in resources and system complexity, the study is not directed towards solving an optimization problem, and therefore, while cost constraints and physical constraints are recognized, they are not explicitly addressed.

3.3.3 Security

The study assumes that information will be protected by the maintenance system "as required" and that technology and safeguards are in place to ensure such protection. No effort is made to address the implementation of security controls.

3.4 Open Issues

The time and resource constraints on the execution of the study left a number of open issues regarding the integrated maintenance system and the IMMOC.

3.4.1 Funding Appropriation, Authorization, and Reporting

Ordinarily, government funding has a number of constraints, including the years in which its spending is authorized, the types of things the money can be used to acquire, the organizations that can receive the money, when the money is available, and the reporting associated with the money. Tracking of funding to be compliant with federal and subordinate regulations is beyond the scope of this effort.

3.4.2 Horizontal Work Transfer Implementation

An open issue with depots is the decision on how to escalate workloads received from a "peer" depot. Since they may not share the same next level node the question is should the depot currently doing the work escalate to its parent or should it return the workload to the peer and then have that peer escalate? Note this is still an issue even if the depots both share the same parent (because of cost associated with the relaying of the workload this may involve us extending the work package concept we discussed last weekend to include an "on behalf of concept". Is the "history" concept is sufficient or not if one keeps with standard shipping and work order terminology as identified within ITIL.

3.4.3 System Scalability Issues

All systems face scalability issues in terms of the constituent hardware, software, and transaction workflow that occurs within the system boundaries. The IMMOC faces several unique scalability issues that are not of the common hardware and software performance variety. Rather, these scalability issues are the result of the IMMOC mission, whether Overwatch or Command and Control and the security requirements to protect classified information.

3.4.3.1 Number of Systems Serviced and Sites Monitored and Controlled

$$S = \sum_{n=0}^{2} d_n f_n$$

Equation 1: System Data Scaling as a Function of Node Count

The most obvious driver of system scalability is the number of operational systems and maintenance sites. As the number of sites grows, then the data set collected grows as a linear multiple of the number of each kind of site. Since the IMMOC primarily monitors four kinds of sites – operational, depot, factory and support – the growth in data can be expressed as an equation. In this equation the system data size (S) is a function of d_n, the size of the data (either in elements or storage requirements) required for an arbitrary facility of type *n,* and f_n, the number of facilities of type *n,* as indicated in Equation 1.

3.4.3.2 Depth of Visibility into Maintenance Mission Execution

The largest driver of system growth, in terms of data elements and the associated infrastructure to transport, process, and store the data elements is the depth of visibility into the maintenance mission execution available to the IMMOC. Each level of detail requires additional data and additional rules to process and display that data, driving not only infrastructure but also system complexity. For example, if the IMMOC tracks only whether a given facility can, in general execute a given maintenance task, then the IMMOC need only receive capability summary data from the facility. If, on the other hand, the IMMOC tracks whether a given facility can, at that moment, support a given maintenance task, then the IMMOC must track all aspects and variables that go into executing that maintenance task, to include space, spare parts, personnel availability, skills availability, funding, and utilities. Further, the business rules that relate the previously enumerated data elements and output the answer are correspondingly complex, taking into account the linkages between the data elements.

3.4.3.2.1 Number of Data Elements

The number of data elements drives both system sizing and complexity issues. Each data element collected serves either as a reportable data element, thereby driving system storage or network performance, or as an element in a calculation, thereby driving processor performance.

Regardless of whether the impact is in storage size, network bandwidth, or processor performance, as the number of data elements increase, so too does the overall complexity of the system. Not only do the physical increases in storage, network, and processor performance drive complexity in terms of requiring more robust subsystems, they also drive cost as subsystems for large-scale execution are often more expensive than those required for small-scale execution.

Finally, as the number of data elements grows, so too grows the number of interrelationships of those data elements with each other, resulting in design complexity.

3.4.3.2.2 Number of System Linkages

The number of system linkages within the maintenance system drives scalability issues through both the Overwatch and Command and Control missions. In the Overwatch mission, a link between maintenances node causes the storage for the data elements associated with a link each link to grow linearly with the number of links. Within the Command and Control mission, the number of links in the maintenance tree increases the complexity of routing decisions and the optimization problems associated with the maintenance system.

3.4.3.2.3 System Update Cycle

System update cycles for data collection drive scalability in a number of ways. Increased sample times increase the fidelity of the data collected and the associated analysis that can be performed. For a given data element, there is a point of diminishing returns at which increased sampling returns no additional data. The primary equation that governs sampling rates is the Shannon Sampling Theorem[2]. Using the Shannon Sampling Theorem, the IMMOC can model the effect of increased data sampling on the precision of the reconstructed signal and compare the information gained to the increased resource requirements.

[2] http://en.wikipedia.org/wiki/Nyquist%E2%80%93Shannon_sampling_theorem

As system updates increase in frequency, the aggregate data transmitted per unit time also increases. This drives commensurate increases in network, processing, and storage capacity to accommodate the data.

Further, as system update cycles increase in frequency, the processing, storage, and transmission capacity of the sensors must also scale to accommodate the increased sample times.

3.4.3.3 Security

The IMMOC, as a DoD system, implements the Bell-LaPadula[3] security model. The Bell-LaPadula security model formalizes in a mathematical construct the security policy contained in Executive Order 12958, as amended by Executive Order 13292, dated 25 March 2003. However, the Bell-LaPadula model does not account for handling caveats that restrict access and implement “need to know” or separation of duties.

As the integrated maintenance system grows and the number of operational systems supported increases, so too does the number of interactions between entities with various roles at various classification levels and handing restrictions.

Further, the assembly of data at one classification level may result in the entire aggregation being at a higher classification. For instance, the location or function of a single computer may not be classified, but the network map containing all of the machines may in fact be classified.

The data aggregation problem may drive the integrated maintenance data processing systems and communications networks to operate at a higher level of classification than the operational systems require. The delta between the highest level of classification of data on the integrated maintenance system and the lowest level of classification of a supported operational system will drive complexity in the security model and implementation. The lack of true multi-level secure systems will drive duplicate infrastructure to process data at various classification levels and to replicate data from lower levels to higher levels so as not to violate the Simple Security Property of the Bell-LaPadula model.

3.4.3.4 Users and Roles

Related to security, but focused on system and data integrity as opposed to data confidentiality, is the notion of users and roles. Users represent a discrete named entity whereas a role represents a function that any number of users could perform. Typically, users are assigned to roles, which are then authorized to perform functions. As the number of systems supported by the integrated maintenance system grows, so too does the number of users and the number of roles.

Further, the matrix that maps users to roles has to be controlled to ensure that business rules are enforced and that a single user is not empowered to bypass the business processes. As the matrix grows in size, the ability to enforce effectively business rules through rules and users decreases without the introduction of automated tools and detailed audits.

[3] http://en.wikipedia.org/wiki/Bell-LaPadula_model

4.0 Integrated Maintenance Mission Goals

This section provides a high-level overview of the processes required to execute the two primary IMMOC missions – Overwatch and Command and Control. Three additional non-mission areas that constrain the IMMOC in executing the Overwatch and Command and Control mission are also addressed: Funding Streams, Quantitative Measures, and Security.

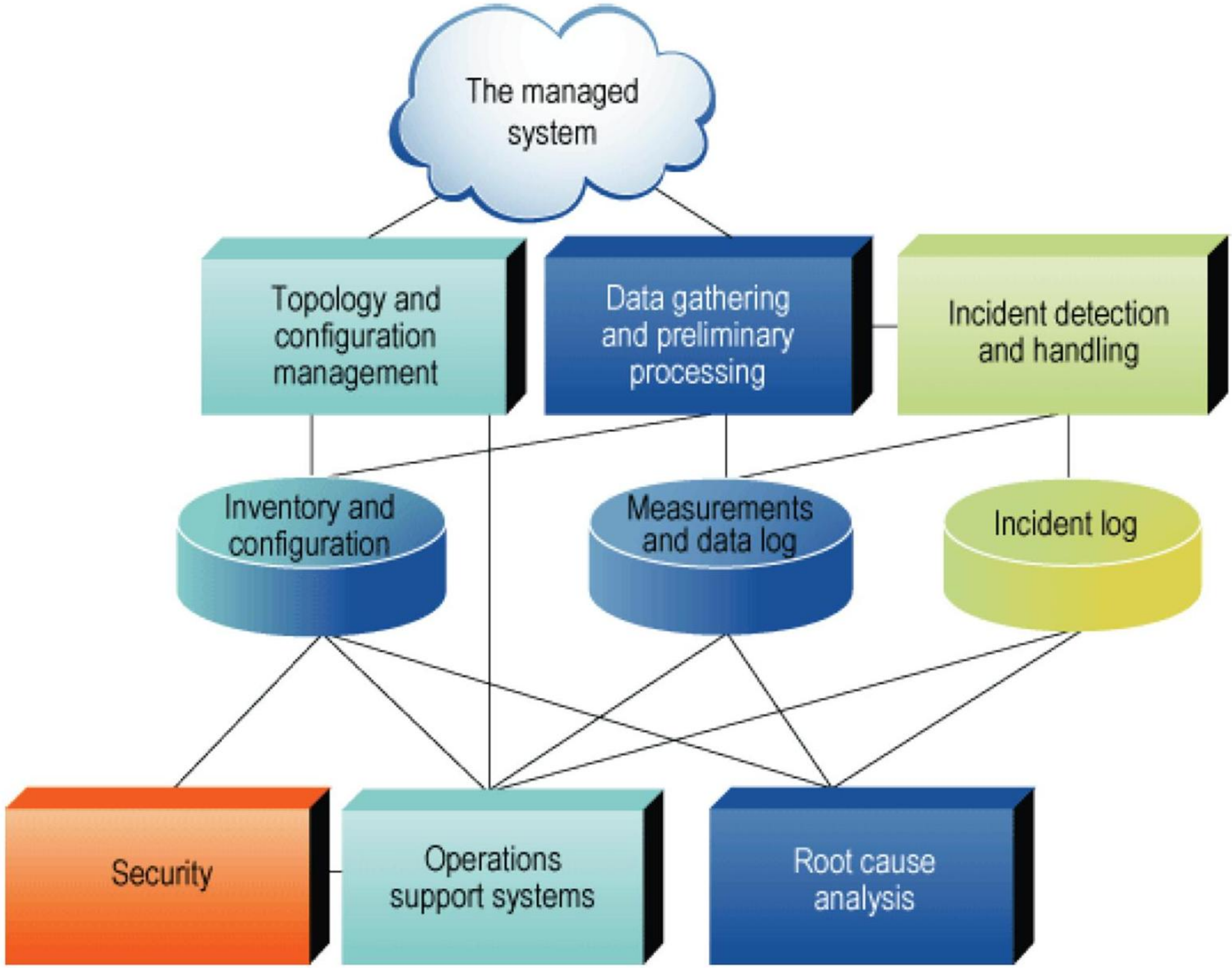

The managed system
Topology and configuration management
Data gathering and preliminary processing
Incident detection and handling
Inventory and configuration
Measurements and data log
Incident log
Security
Operations support systems
Root cause analysis

Figure 4-1: Management System Functions[4]

Leveraging ITIL as a framework, Figure 4-1: Management System Functions illustrates the processes that the IMMOC will perform in the Overwatch and Command and Control missions. The Overwatch mission enables the IMMOC to gather data used to support command decisions related to incident handling, alternate system routings, as well as non-command functions related to data analysis. While not a perfect mapping, the ITIL model can be extended to service providers that have physical in addition to logical resource constraints.

[4] Burton Group: Architectural Overview of Network Management, Version: 1.0, Oct 17, 2005

4.1 Overwatch

To execute Overwatch of the integrated maintenance system, the IMMOC has to be able to monitor the status of all integrated maintenance assets. The depth of insight into asset status governs the precision and detail of the status reporting performed in the IMMOC.

Overwatch presupposes a number of sub-missions. The requirements in this document are based on ITIL standards associated with system monitoring and reporting.

4.1.1 Incident and Problem Management

Execution of traditional service desk functions, including system monitoring, provide data that can be mined and turned into statistics that indicate availability, reliability, and maintainability trends. Analyzing trend data enables design and process refinements (e.g., Lean and Six Sigma) to enhance infrastructure reliability and mission execution. Collected statistics should also enable measurement of each maintenance organization's effectiveness in the execution of maintenance tasks against maintenance service levels subscribed to by various operational systems.

4.1.2 Incident and Problem Management Lifecycle

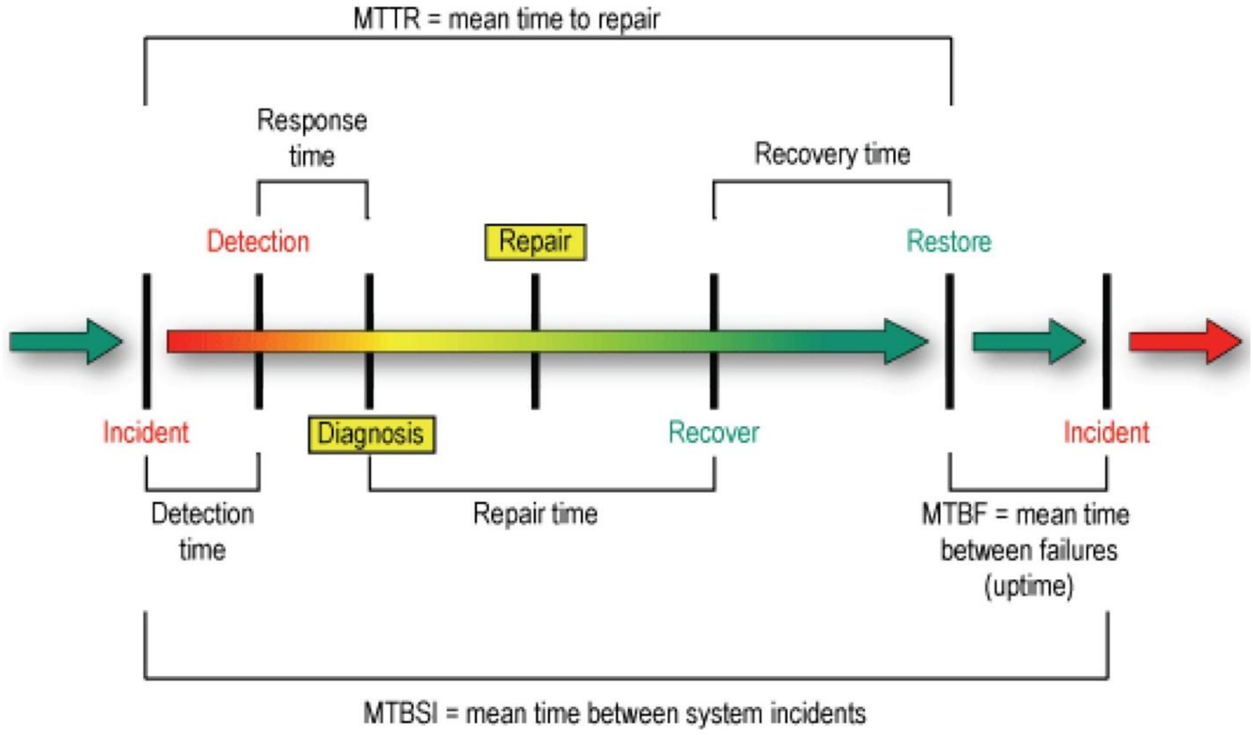

MTTR = mean time to repair
Response time
Recovery time
Detection
Repair
Restore
Incident
Diagnosis
Recover
Incident
Detection time
Repair time
MTBF = mean time between failures (uptime)
MTBSI = mean time between system incidents

Figure 4.1-1: Incident Lifecycle[5]

Incident and problem management are key aspects of a maintenance system. Figure 4.1-1 shows the ITIL representation of the incident and problem management lifecycle. Within the context of the Overwatch mission, the IMMOC is responsible for measuring Mean Time To Repair (MTTR), Mean Time Between System Incident (MTBSI), and Meant Time Between Failures (MTBF) for both the components of the integrated maintenance system, to include the IMMOC

[5] Burton Group: The IT Infrastructure Library: Supporting the Service Chain Version: 2.0, Dec 05, 2005

itself, as well as for the operational systems supported by the integrated maintenance system. While beyond the control of the IMMOC to directly influence from the Overwatch mission (but not the Command and Control mission, via directed maintenance actions), MTBSI, MTTR, and MTBF provide valuable metrics for capacity planning and demand forecasting. Additionally, time-based metrics provide the baseline against which process improvement activities are measured.

4.1.3 Incident Management

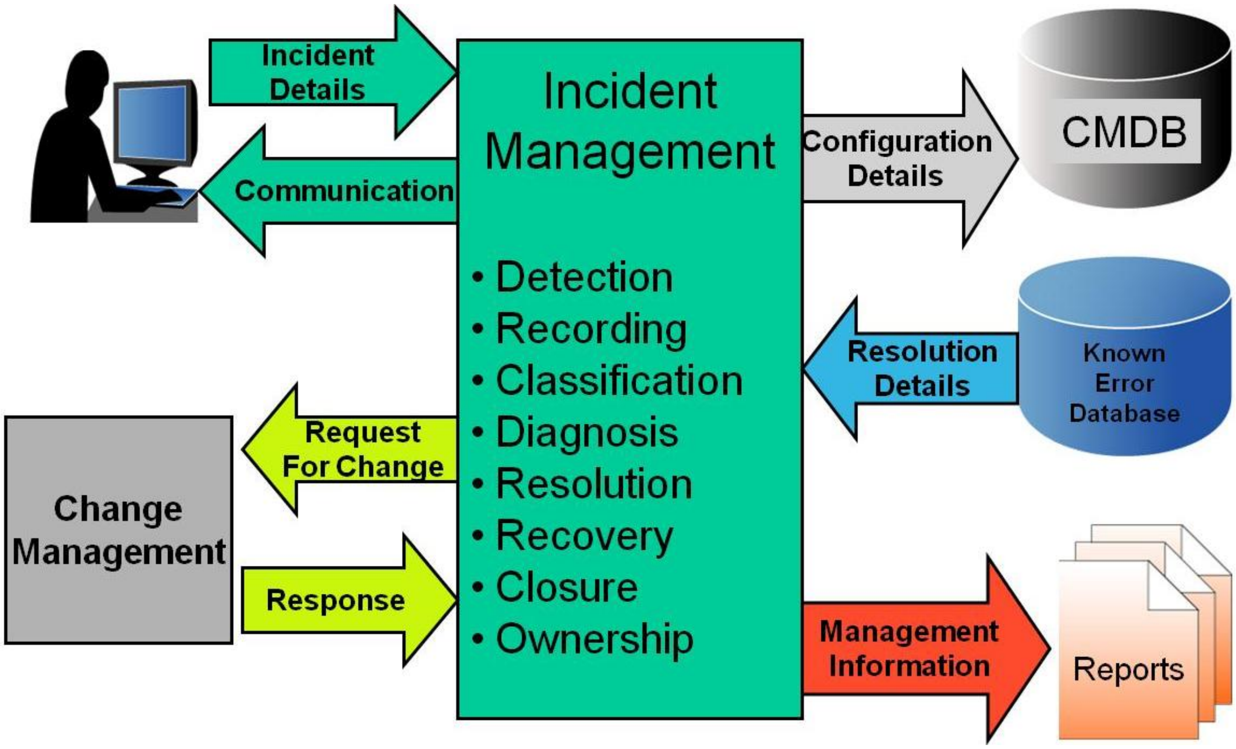


Figure 4.1-2: Incident Management Data Flows[6]

The incident management process, illustrated in Figure 4.1-2 shows the ITIL representation of the incident management lifecycle as well as the data flows within the lifecycle. As with incident and problem management time-based metrics, the IMMOC must execute the incident management lifecycle for both the integrated maintenance system and the operational systems supported. The ITIL definition of incident management provides a framework for defining maintenance actions (incidents) as a service and the wherewithal for measuring that service. The lifecycle also enables process improvement using the known error database and the configuration details of existing systems.

Incident management represents the primary function of the integrated maintenance system from the perspective of the operational system.

[6] Burton Group: The IT Infrastructure Library: A Service Perspective, September 15/16, 2005

4.1.4 Problem Management

Within ITIL, problems are incidents that affect operations. Problem management requires the restoration of the system to an operational state. As Figure 4.1-3 shows, problem management entails significant information flows in addition to the actual maintenance task execution and workflows that are not pictured. Although Figure 4.1-3 does not address the actual execution of the maintenance tasks, it does show the core of the integrated maintenance mission – namely, the management of the maintenance process. The existing maintenance segments integrated within the existing systems today are capable of executing the maintenance tasks. However, management of the maintenance tasks in order to reduce costs and ensure maintenance of service levels is what distinguishes the integrated maintenance mission from the vertically integrated maintenance tasks.

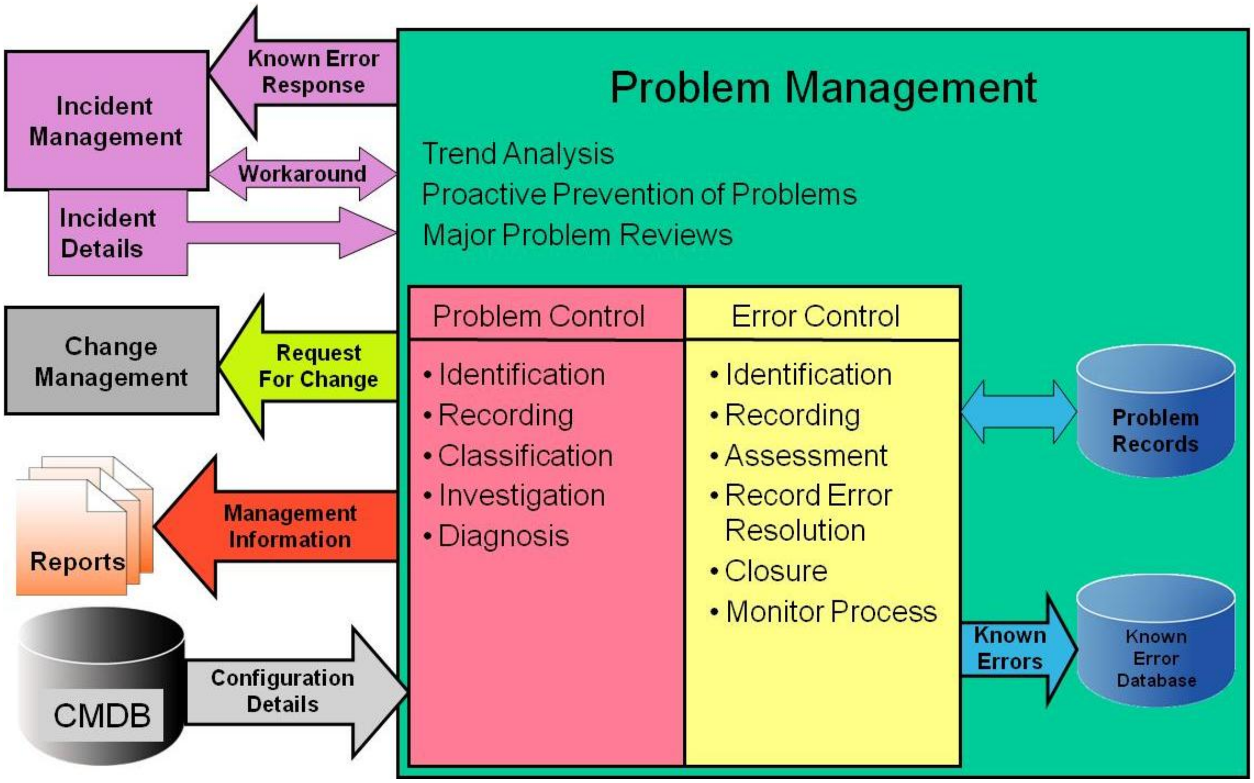


Figure 4.1-3: Problem Management Information Flows[7]

4.1.5 Incident or Problem and Availability Monitoring and Metrics

Within the lifecycle of an incident or problem, there are opportunities to reduce downtime by minimizing the time needed to return the system or service to operational status. The lifecycle[8] for downtime typically involves detection, diagnosis, repair, recovery (i.e., recover lost data), and restoration.

[7] Burton Group: The IT Infrastructure Library: A Service Perspective, September 15/16, 2005
[8] Burton Group: The IT Infrastructure Library: Supporting the Service Chain Version: 2.0, Dec 05, 2005

4.2 Command and Control

At the core, Command and Control is about managing a system to execute a mission. As ITIL is a recognized best practice for service management, and the integrated maintenance system provides maintenance services, the ITIL framework has been used to describe the two IMMOC missions of Command and Control.

4.2.1 Capacity Management

Capacity Management is the process of ensuring the "best use of the appropriate IT infrastructure to cost effectively meet business needs by understanding how IT services will be used and matching IT resources to deliver these services at the agreed levels currently and in the future[9]."

Effective capacity management balances cost and capacity with supply and demand, ensuring that the capacity of the maintenance infrastructure (communications facilities, logistics, personnel, processing, spares, and tooling) provides the most efficient use of available resources and can be cost justified as supporting the operational system maintenance requirements within established service levels. Under-capacity can cause performance problems that impact the ability of the maintenance system to sustain systems at the desired operational effectiveness and availability. Overcapacity increases the cost of delivering services without offering commensurate value in new services or service execution for the money spent although it does increase the guarantee that maintenance will be delivered within the agreed to levels of service.

Capacity Management not only ensures optimal performance and utilization of the existing infrastructure, but also ensures optimal planning for future infrastructure investments relative to mission imperatives. Without a deep understanding of how the infrastructure currently supports the maintenance mission and how the maintenance mission – and the associated impact to infrastructure – is likely to change in the future capacity management cannot be properly executed. Understanding is critical to modeling, and therefore the ability to optimize the planning, acquisition, and building of new infrastructure to meet future needs.

4.2.1.1 Capacity Management Activities

Capacity management is more than planning for adequate maintenance infrastructure (communications facilities, logistics, personnel, processing, spares, and tooling) to handle the defined workload. Rapid technological advances have a direct bearing on the maintenance services offered, whether in terms of reduced costs, reduced MTTR, enabling a lower echelon maintenance facility to execute the maintenance function than was previously possible, enabling remote maintenance, or enabling new concepts such as enhanced preventive maintenance or enhanced system self-diagnostic capabilities. However, not all innovations will save money or increase productivity. Which innovations can result in improved performance can only be answered in the context of current operational metrics and requirements.

Capacity Management has three primary subordinate processes10, as illustrated in Figure 4.2-1:

- Business Capacity Management looks to the future and understands the evolving needs of the maintenance enterprise. The primary function of Business Capacity Management is to plan and implement sufficient capacity to support systems that will be operational one to

[9] Burton Group: The IT Infrastructure Library: Supporting the Service Chain Version: 2.0, Dec 05, 2005
[10] Burton Group: The IT Infrastructure Library: Supporting the Service Chain Version: 2.0, Dec 05, 2005

three years in the future. Inputs to Business Capacity Management can include existing Service Level Agreements (SLA), future SLRs, business plans, and the Capacity Plan.

- Service Capacity Management is focused on current operations and has a deep understanding of usage patterns, available resources, and SLAs. Inputs to Service Capacity Management include SLAs, performance reports, tuning reports, and Demand Management reports.
- Resource Capacity Management (RCM) looks at optimizing the use of all the current components of the maintenance infrastructure. This subordinate process also monitors system deployments and technological advances and determines the impact of new systems and technologies to the maintenance infrastructure. Inputs to RCM are evaluations of future system operational dates, current technology and its utilization within the maintenance infrastructure, future or alternate technologies and their potential application within the maintenance infrastructure, and changing business requirements.

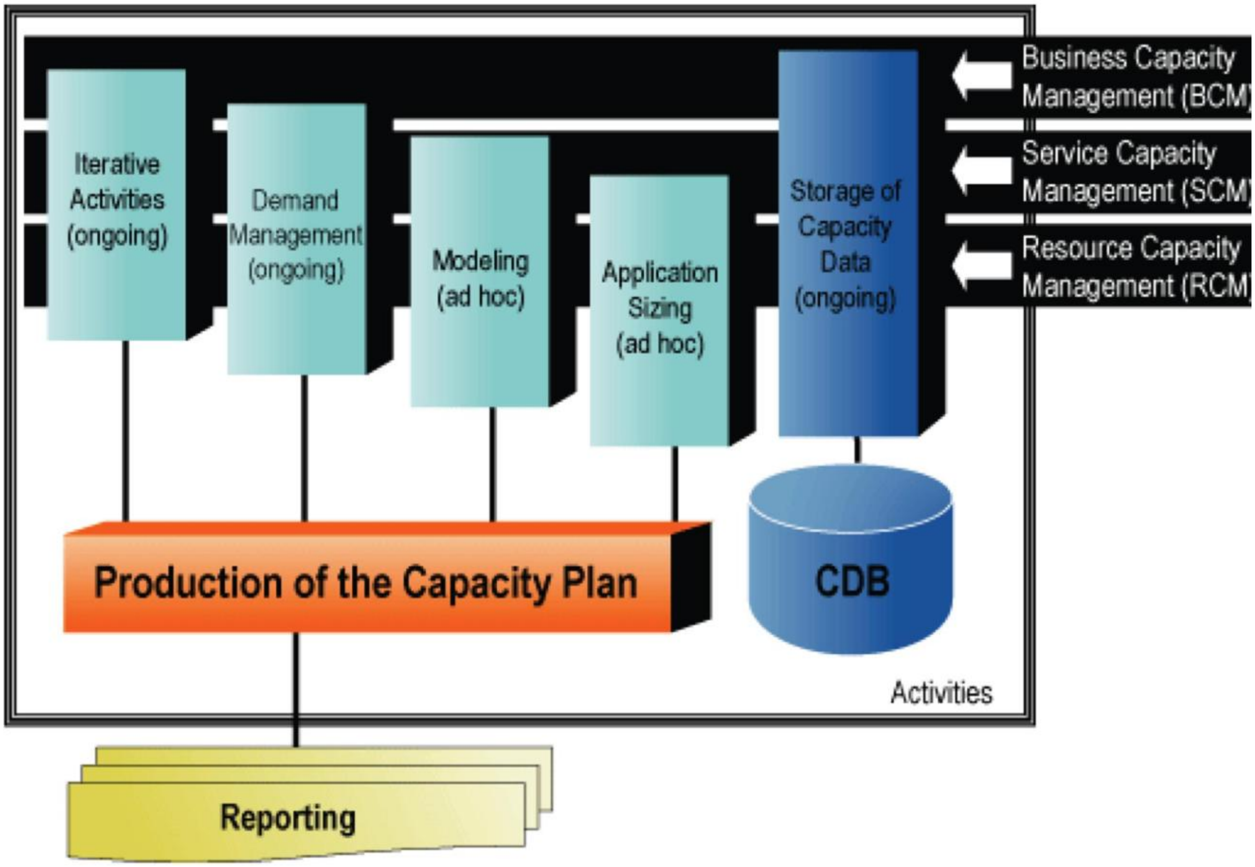

Business Capacity Management (BCM)
Service Capacity Management (SCM)
Resource Capacity Management (RCM)
Iterative Activities (ongoing)
Demand Management (ongoing)
Modeling (ad hoc)
Application Sizing (ad hoc)
Storage of Capacity Data (ongoing)
Production of the Capacity Plan
CDB
Activities
Reporting

Figure 4.2-1: Capacity Management Activities Planning and Execution[11]

In ITIL, Iterative Activities are also known as Performance Management. Performance Management consists of the daily infrastructure monitoring to ensure optimum operation and prevent service interruptions. The major Performance Management activities are:

[11] Burton Group: The IT Infrastructure Library: Supporting the Service Chain Version: 2.0, Dec 05, 2005

- Monitoring the infrastructure and supporting performs to ensure that SLAs are met. Monitoring includes response time, throughput, and other metrics based on thresholds set by SLM.
- Analyzing utilization trends and service levels to establish and measure baselines against system performance. Baseline comparisons allow operators to identify exception conditions and noncompliance with the SLAs. Additionally, trend lines can forecast resource usage and compare actual against predicted growth, to facilitate capacity planning.
- Tuning adjusts operational parameters to improve system and service performance.
- Implementing tuning measures through the Change Management process to minimize service disruptions and ensure configuration management control.

4.2.1.2 Demand Management

Demand Management influences service and infrastructure usage in accordance with business priorities by limiting the quantity of services available to any customer. Demand Management is the most cost-effective form of short-term Capacity Management[12].

One form of Demand Management is chargeback, in which the consumer is charged for the consumption of the service. Chargeback can price resources according to time of day or utilization to encourage off-peak usage. However, differential pricing requires knowledge of schedules, peak activity times, and normal usage patterns, which can only be established by measuring performance over time. Additionally, Demand Management may cause customers to alter work patterns and shift workloads to other resources or other times, and therefore should not be imposed without prior coordination with system users.

4.2.1.3 The Capacity Database

The Capacity Database (CDB) is part of the ITIL Configuration Management Database (CMDB) and contains data relevant to Capacity Management. The CDB is conceptually a single database, although it may be created from a federation of databases related to capacity information.

The CDB includes business information, financial data, service reports, technical specifications, and utilization data from which management reports, the Capacity Plan, and technical reports.

4.2.1.4 Modeling

Modeling is the act of creating a logical representation of the baseline system that behaves in a manner similar to the actual baseline system. A model enables the behavior of the infrastructure to be predicted under normal and exceptional conditions or under user-defined conditions. Ultimately, the utility of modeling enables feasibility and capacity planning studies without building an experimental system or running tests on the operational system.

Five modeling techniques[13] are shown below in order of increasing cost, accuracy, and complexity:

1. Estimation is the least costly technique. It is based on previous experience and current knowledge. Estimation is not terribly accurate and is mainly useful for small, routine issues.

[12] Burton Group: The IT Infrastructure Library: Supporting the Service Chain Version: 2.0, Dec 05, 2005
[13] Burton Group: The IT Infrastructure Library: Supporting the Service Chain Version: 2.0, Dec 05, 2005

2. Trend analysis involves the use of resource utilization and performance data collected over a period and is generally presented in graphical form. Trend analysis is slightly more sophisticated than estimation, and although it can provide better results, it is mainly useful for modeling short-term activities. Trend analysis can be considered an educated estimate.
3. Analytical modeling uses more sophisticated tools than trend analysis, such as mathematical models. These models are generally tailored for specific components, systems, or services and, therefore, do not give a view of the entire service chain. Although these tools need regular updating to reflect new equipment, services, and applications, they are generally less expensive and take less time than simulation modeling.
4. Simulation modeling compares discrete events (e.g., loading peaks and component failures) against a specific infrastructure configuration. Simulation is normally performed in a dedicated laboratory environment or using tools that simulate transactions and network traffic.
5. Benchmarking is the most expensive, yet most accurate, form of modeling. Benchmarking creates a duplicate operational environment or models the actual operational environment for testing. Workloads are replicated and the impact on this mirror environment is observed and measured. Operational variables (e.g., bandwidth and CPU performance) are then altered and the actual effect recorded. Benchmarking removes most of the guessing, because it uses the entire infrastructure in its simulations. Benchmarking will also prove whether the current infrastructure can support planned growth.

4.2.2 Service Routing

Service routing is the function of Command and Control that enables work packages to flow along ad hoc or non-default paths through the maintenance system. Service routing requires the Overwatch mission to be successfully executed, as system status and resource utilization knowledge is necessary to ensure that the alternate routing can be accomplished within the work package constraints (e.g., funding, security, timing) and existing workloads.

Service routing enables work packages to transit over secondary pre-established links or to make use of ad hoc links that the IMMOC establishes. Ad hoc link creation is a subfunction of the service routing function. Ad hoc links can be either logical communication paths, physical logistics paths, or the re-routing of an existing logistics path (e.g., changing the routing of a truck to an alternate destination.

4.3 Funding Streams

Each operational system currently funds its own maintenance segment. As the primary source of funding, the operational system has control over the execution of maintenance actions, which are then optimized relative to the priorities and funding constraints of that particular system. Further, each operational system is responsible, within the appropriate rules, regulations, and laws, for reporting on the disposition and allocation of funding across all operational, maintenance, and contractual tasks. Within the integrated maintenance system, the maintenance system exists as a service provider to operational systems. Two paradigms exist for funding the integrated maintenance system. In paradigm one, funding is authorized in the same manner as for operational systems and the integrated maintenance system executes within the confines of that budget. The second paradigm is a fee for service organization in which the integrated maintenance system is established as a working capital fund or other entity that is able to charge for services. Within the second paradigm, there are two subcategories:

- Fee for Service: Flat rate buys into the IMMOC, with additional fees per incident
- Pre-paid Service Level Agreement: Flat rate for all service – better funding

Integrated maintenance funding can occur from either or a combination of the funding paradigms.

Further, in accordance with public law and budget priorities, the integrated maintenance s system may have to track and account for individual funding streams, as congressionally authorized funding streams may be required, by law, to be spent in support of a particular system or may be prohibited from being spent in support of particular systems. Regardless of the constraints, it is the responsibility of the IMMOC to account for, and report on the status of funding streams and ensure compliance with all applicable laws and regulations.

4.4 Quantitative Measures

As a concept, the primary measure of effectiveness of the integrated maintenance system is whether the integrated maintenance system can perform better than the existing stovepipe maintenance segments embedded within operational systems. The definition of better may vary between stakeholders in its specific measurement and definition for threshold values, but ultimately enables a comparative assessment that evaluates the effectiveness of the integrated maintenance system as compared to the existing maintenance segments.

Effectiveness can be measured in ITIL standard terms related to cost, throughput, utilization, “customer” satisfaction, and service-level agreements. Alternate measures of effectiveness may include insight and oversight of the maintenance functions and cost, improved adherence to security regulations, or greater resilience within the maintenance system to failures that could impact operational systems. Additionally, effectiveness can be measured in terms of political goals such as maintaining industrial base, congressional districts in which work is performed, and alignment with the Base Realignment and Closure (BRAC) Commission.

4.5 Security

Space-based systems such as AEHF, DMSP, DSP, GPS, MILSTAR, SBIRS, and TSAT operate at multiple levels of classification, from UNCLASSIFIED to TOP SECRET as defined in Executive Order 13292[14]. For example, GPS provides UNCLASSIFIED 10-meter geolocation service to civil users, however at higher classification levels GPS provides greater accuracy in both geolocation and temporal location. Similarly, while “fact of” TSAT is UNCLASSIFIED, the capabilities and vulnerabilities of the TSAT system are classified.

Not only do mission capabilities occur at multiple classification levels, but so too do components that the integrated maintenance system will service and the IMMOC will monitor. For example,

[14] http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html

the ground station for TSAT may make extensive use of the Oracle™ suite of software; however, the fact that TSAT is using Oracle products may be classified[15].

Other examples of data at multiple classification levels may include operational and development locations. While it is public knowledge that Lockheed Martin Corporation is the prime contractor for the TSAT system, the location of the ground stations and maintenance sites is classified.

There are many reasons for classifying data, many of which are also classified. However, some reasons for having data at multiple classification levels include:

- Protection of sources and methods for sensor platforms: identifying the specific capabilities of a particular sensor suite (SBIRS, DSP) enables the targets of those sensor systems to take steps to deny collection of deceive the collectors
- Protection of system vulnerabilities: identifying specific products or components may allow adversaries to identify vulnerabilities in the components, increasing the ability of adversaries to defeat or even destroy the system
- Protection of communications links: identifying the communications parameters may allow adversaries to collect intelligence from or jam communications links

Regardless of the reason, the IMMOC and the integrated maintenance system operate in a multilevel environment governed by DoD and Intelligence Community standards.[16] Therefore, the processing systems and communications networks need to provide appropriate protections for each classification and handling caveat[17] combination possessed by data moving through the integrated maintenance system.

Therefore, each data element, as well as each user, computer and communications link needs to possess security attributes, including clearance (or classification level) and need to know (or handling caveats). Users are allowed to access and computers and networks allowed to process and transport data whose security markings meet two characteristics: (1) the classification of the data is less than or equal to that of the user, network or computer; and (2) the handling caveats on the data are a subset of the handling caveats available to the user, network, or computer.

Multi-level security, outside of system-high processing, remains a topic of active research in academia, network vendors, hardware vendors, operating system vendors, government agencies, and systems integrators.

[15] Use of Oracle in this example is notional and is provided simply as reference for discussion, not as an endorsement or identification of a specific product used within TSAT.

[16] DoDD 8500.1, DoDD 8500.2, and DoDI 8510.b govern DoD multi-level systems while DCID 6/3 govern intelligence systems.

[17] EO-12958 describes the three classification levels identified by law. Handling caveats, however, create mandatory controls for enforcing need to know.

5.0 IMMOC Mission Execution

The IMMOC is an integrated element that provides a real-time network and system information and control mechanisms to ensure completion of the maintenance missions as defined in the maintenance concept for a given system. The IMMOC comprises the hardware and software tools, personnel, and processes used to monitor, manage, and control the maintenance mission.

The IMMOC executes two primary missions with respect to the maintenance mission: Overwatch and Command and Control. Overwatch is defined as the aggregation of operationally relevant data into the IMMOC for the purposes of informing commanders and other stakeholders as to the mission status of the maintenance mission and the components that execute that mission. Overwatch is a view-only capability that does not provide the means for directing action. Command and control, on the other hand, provides the means for IMMOC commanders to direct the execution of the maintenance mission by issuing commands to maintenance mission operational components.

Per the sponsor-provided CONOP, the IMMOC will provide continuous, centralized maintenance mission support and delivery for supported systems.

As a command center, the IMMOC provides centralized monitoring, performance analysis, fault isolation, maintenance coordination, intrusion detection, configuration management, and system administration of the maintenance mission components. Primary IMMOC functions include incident management, network operations and management, performance analysis, fault resolution, maintenance coordination, configuration management, system administration, and security management. Additionally, the IMMOC will participate in problem, change, availability, release, service continuity, service level, and capacity management functions as necessary.

5.1 Overwatch

The Overwatch mission is the basic mission of all operations centers. Fundamentally, overwatch consists of gathering data from operational entities and presenting that information to stakeholders in some manner for the purposes of reporting. Overwatch does not imply mission management or command of the elements that provide data.

The stereotypical Overwatch display is the stoplight chart of red, yellow, and green used throughout the operations center world to denote levels of mission readiness or problem severity. Ideally, the Overwatch system allows both aggregation and disaggregation of data to allow reporting data to be examined at arbitrary levels of detail. Further, the ability to aggregate data enables the construction of business process rules that allow for status reporting that is not based on hierarchical decomposition of data. For instance, in a physical decomposition model, all components are rolled up into the status of each facility. However, a well constructed Overwatch system will allow the disaggregation of data from the facility to allow the display of component status across facilities, enabling deeper levels of understanding. These non-hierarchical status displays should be user-definable in accordance with business process and rules to ensure the maximum flexibility of the system.

Based on the IMMOC requirements documents, the Overwatch mission consists of monitoring all maintenance-relevant systems at all maintenance mission sites. To execute this mission, the IMMOC needs to monitor numerous subsystems at and across mission sites. The IMMOC is dependent on the mission sites to provide the data for monitoring purposes, and therefore will need to have a Memorandum of Understanding (MOU) or equivalent in place with each maintenance site. Data to be monitored includes the status of:

- Communications links
- Computing systems
- Facility status
- Financial systems
- Logistics systems
- Maintenance operation systems
- Mechanical systems
- Personnel systems

The goal of the IMMOC is to assemble the status data, hereafter referred to as telemetry, into a comprehensive picture as to the state of health of the maintenance segment supporting the mission system.

5.2 Command and Control

Command and control is defined as:

> The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission[18].

In the context of the maintenance mission, the IMMOC is the properly designated commander and the maintenance sites are the assigned and attached forces. The mission is to optimize the execution of the maintenance mission to ensure the operational availability of the mission system. The maintenance mission Command and Control functions can be divided into three functions – alternate routing, mission allocation, and mission planning and scheduling.

5.2.1 Alternate Routing

Alternate routing commands enable the IMMOC to redirect a work package from its previously scheduled workflow to a new workflow and new service queues. The work package can be physical, such as the allocation of a spare from Depot B instead of Depot A or logical, such as the direction to use communications link B instead of A for a given data transfer. In either case, the IMMOC provides new orders, or commands, to the subordinate elements to effect the redirection. Redirection allows the IMMOC to implement a priority-based resource allocation policy, ensure service levels are met, respond to outages, and potentially hide information from those who do not have a need to know, thereby enabling compliance with Executive Order 13292.

[18] US Army Field Manual 3-0, Operations: http://www.dtic.mil/doctrine/service_publications_usarmy_pubs.htm

5.2.2 Mission Allocation

Mission allocation is similar to alternate routing, except that it is the initial routing command. When a maintenance request arrives for processing within the IMMOC work queue, the IMMOC allocates that task, based on the current system status, to a specific workflow and set of work queues. Once the mission has been allocated, commands are sent to the appropriate sites for implementation and the system status is updated to reflect the new work package.

5.2.3 Mission Planning and Scheduling

Mission planning and scheduling is the highest level of Command and Control that the IMMOC can perform. Mission planning and scheduling is the function that enables the IMMOC to optimize resources during execution of the maintenance mission and ensure that the maintenance system can support current and projected maintenance requests. Without an ability to plan and schedule maintenance tasks, the IMMOC can only react to maintenance tasks; it cannot proactively allocate resources to ensure optimal usage. Mission planning and scheduling combines system status with historical data and models.

6.0 Analysis

The integrated maintenance system architecture encompasses aspects of the physical, logical, and functional integrated maintenance system architecture as well as the physical, logical, and functional aspects of the command center.

Prior to establishing architectural representations that satisfy the requirements and intent, as embodied in the MMOC CONOP provided by the project sponsor, it is necessary to baseline the graph that represents the maintenance system. Once the maintenance system has a baseline representation, the interaction of the IMMOC with the maintenance system can be captured.

6.1 Integrated Maintenance System First Level Architecture

This section presents a representation of candidate first-level architecture for the integrated maintenance system to establish system boundaries and first-order relationships between the integrated maintenance system and external systems as well as the relationships between major subsystems within the integrated maintenance system.

The first level architecture establishes and defines the terms of reference for the integrated maintenance study with respect to the IMMOC and the integrated maintenance system.

6.1.1 Integrated Maintenance System Context

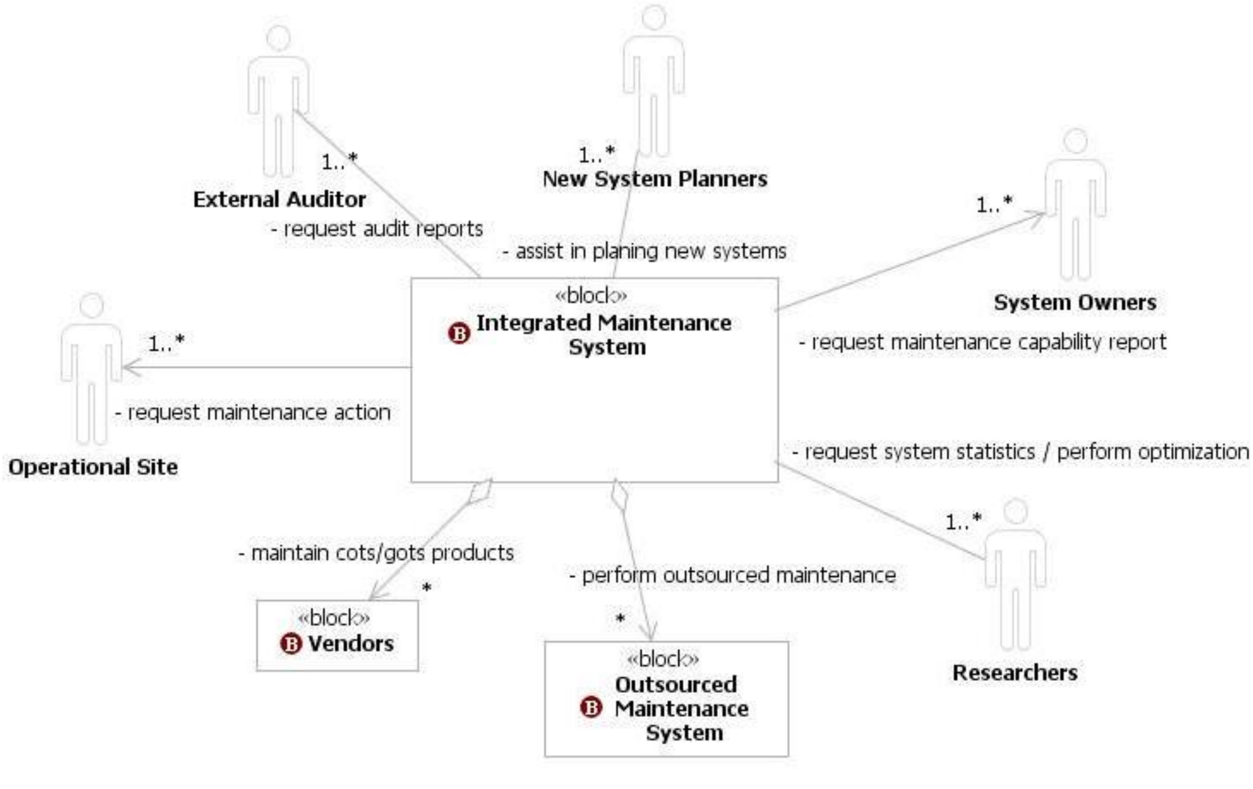

External Auditor
1..*
- request audit reports
New System Planners
1..*
- assist in planing new systems
System Owners
1..*
- request maintenance capability report
«block»
Integrated Maintenance System
Operational Site
1..*
- request maintenance action
- request system statistics / perform optimization
Researchers
1..*
- maintain cots/gots products
*
«block»
Vendors
- perform outsourced maintenance
*
«block»
Outsourced Maintenance System

Figure 6.1-1: Integrated Maintenance System Context Diagram

Figure 6.1-1 establishes a visual context to describe the context in which the integrated maintenance system operates. Its purpose is to identify the boundaries of the integrated maintenance system as well as to identify primary relationships with external systems and entities as well as the intended purpose of the relationship.

6.1.1.1 Diagram Definitions:

6.1.1.1.1 Operational System

This refers to any operational system that receives maintenance from the integrated maintenance system. The primary interaction with the integrated maintenance system will be through maintenance actions that requested from the integrated maintenance system and the over watch mission requirement 4.5.1.

6.1.1.1.2 External Auditor

This refers to any entity that has the authority to request/perform an audit of the integrated maintenance system or the records of any system maintained by the integrated maintenance system. These are listed as a primary relationship in support of requirement 4.5.2.

6.1.1.1.3 New System Planners

This refers to any entity that is using the integrated maintenance system to perform either capacity planning for a current system or developing a new system. It is the intent that the integrated maintenance system will assist in providing maintenance plans and estimates for the new system. This will allow the integrated maintenance system to perform capacity-planning activities as well as support the organizational requirements 4.1.1 and 4.1.2.

6.1.1.1.4 System Owners

This refers to any entity that has control over either the integrated maintenance system itself or any system maintained by the integrated maintenance system. System owners along with the Operational Site represent the primary interactions for the over watch mission requirement 4.5.1.

6.1.1.1.5 Researchers

The represents any entity that is performing research/analysis on either maintenance processes or the policies of the integrated maintenance system itself allowing cross system analysis that is not possible in a stovepipe maintenance process. This is in keeping with best practices that will allow integrated maintenance system to optimize its services as identified in requirements 4.5.1.3 and 4.5.1.2.

6.1.1.1.6 External Vendors

This represents the COTS or GOTS vendors that are the ultimate ends for any COTS or GOTS components included in the maintained systems. Due to the increasing use of COTS or GOTS products in operational systems, this ensures that their ability to include COTS or GOTS maintenance trails as needed, per requirement 4.4.2.

6.1.1.1.7 Outsourced Maintenance Systems

This represents any maintenance activities that are not performed by the integrated maintenance system or the original vendor. It is intended to support future growth and as well as to differentiate COTS or GOTS maintenance trails from internal government maintenance trails (for example for crypto modules)

6.1.1.2 System Context

Figure 6.1-2 is a Level-0 decomposition of the integrated maintenance system. The term Level-0 is used because Figure 6.1-2 does not decompose the integrated maintenance system but rather establishes the system as an entity, and secondly establishes what exists outside of the system. Further diagrams will decompose the system into subsystems and assign functions to those subsystems as well as clearly indicate the relationships between the subsystems.

In this architecture, actors (indicated by the 웃 icon) are distinguished from external systems (indicated by a block entity). Actors are capable of using the system to achieve some goal or to obtain a product. Accordingly the operational site is shown as an actor not a external system because it is not only capable of using the integrated maintenance system (via requested maintenance actions) it is also capable of executing some level of control over the integrated maintenance system (for example by allowing or disallowing a scheduled maintenance because of operational considerations). While system planners, researchers, and auditors are not directly able to execute any control, they consume data created by the system and use the system for mission objectives. External auditors use the system to ensure compliance with appropriate DoD and government directives and regulations; as well as to monitor funding and other resource utilizations. System planners will use the system to ensure that maintenance will be available for future systems as well as to provide a feedback from the maintenance knowledgebase.

Researchers will be able to utilize the system not only to compare system performance to applicable commercial activities and identify best practice changes but also to identify and recommend optimizations to the internal activities of the integrated maintenance system. Finally, by explicitly including vendors and outsourced maintenance the architecture makes it clear that some maintenance activities will fall outside its purview and will require interfaces to entities that are capable of performing the maintenance action.

6.1.2 Integrated Maintenance System Internal Structure

Figure 6.1-2: Integrated Maintenance System Internal Block Diagram is a 1st level decomposition of the integrated maintenance system. For the sake of clarity, some infrastructure and supporting subsystems have been omitted. Relationships between the subsystems are indicated with a solid line connecting the two subsystems. For readability reasons some relationships have been omitted.

The 웃 icon represents a subsystem that is the interface for an actor identified on Figure 6.1-2.

The ▤ icon represents an internal subsystem to the integrated maintenance system.

A subsystem with a dashed rather than solid line indicates that the subsystem is an interface to some external entity.

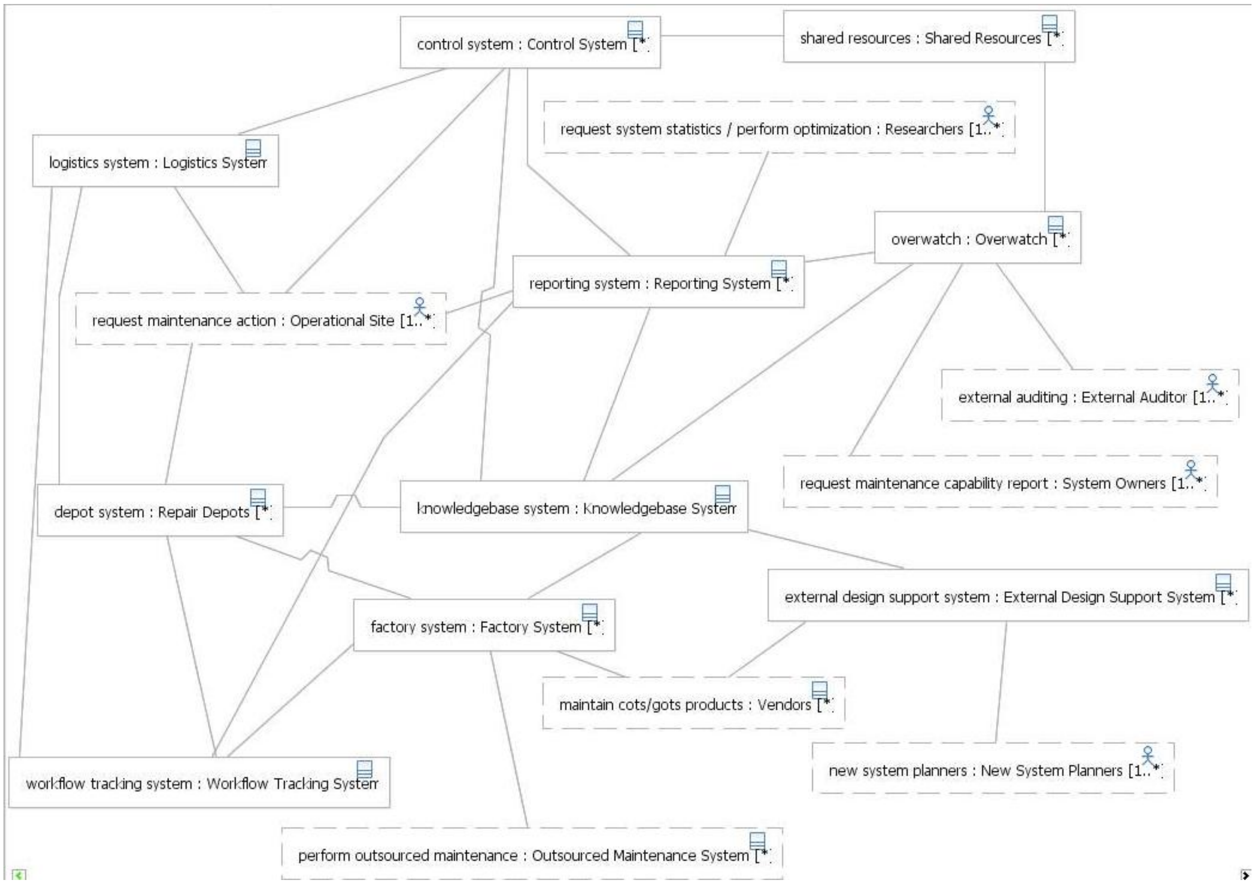

control system : Control System [*]
shared resources : Shared Resources [*]
request system statistics / perform optimization : Researchers [1..*]
logistics system : Logistics System
overwatch : Overwatch [*]
reporting system : Reporting System [*]
request maintenance action : Operational Site [1..*]
external auditing : External Auditor [1..*]
request maintenance capability report : System Owners [1..*]
depot system : Repair Depots [*]
knowledgebase system : Knowledgebase System
external design support system : External Design Support System [*]
factory system : Factory System [*]
maintain cots/gots products : Vendors [*]
new system planners : New System Planners [1..*]
workflow tracking system : Workflow Tracking System
perform outsourced maintenance : Outsourced Maintenance System [*]

Figure 6.1-2: Integrated Maintenance System Internal Block Diagram

6.1.2.1 Interfaces:

All external entities will have an interface into the integrated maintenance subsystem. These interfaces have responsibility for performing the following three functions

1. Restrict access to internal resources and data as specified by applicable operating policy.
2. Provide any data conversion / formatting needed to provide information to the external entity as required as well as to accept information from the external entity
3. Provide presence information on both requested/provided data and the external entity.

6.1.2.1.1 Communications Subsystem

This subsystem is responsible for control over all communication pipes (both logical and physical) used by the integrated maintenance system.

6.1.2.1.2 Control Subsystem

This subsystem is responsible for the C2 component of the integrated maintenance system. In addition to coordinating external commands from either operational systems or system owners the control subsystem is capable of positive control to ensure proper functioning of the integrated maintenance subsystem. This includes but is not limited to actions such as automatic rescheduling of work based on resource availability and initiating surge actions.

6.1.2.1.3 External Design Support Subsystem

This subsystem is intended to support both the integrated maintenance system in its capacity planning and integration with COTS and GOTS products in addition to providing analysis capability to the New System Planner Interface.

6.1.2.1.4 External Auditor Interface

This subsystem is responsible for interfacing with external auditors and law enforcement / investigative agencies. From the perspective of the integrated maintenance system the only difference between a request from an external auditor and one from a law enforcement or investigative agency is the scope and level of detail available to the requestor. Because all interfaces restrict access based on operational policy there is no need to provide a separate interface to support these two entities. This interface will not be responsible for the data generation or aggregation of the information requested, instead it will rely on the reporting subsystem and appropriate shared resources to provide the necessary data. The interface will provide presence data for both the external users as well as the requested data. This interface provides both real time and non real time data and status as determined by operating policy.

6.1.2.1.5 Factory Subsystem

This is the logical representation of factories in the integrated maintenance system.

6.1.2.1.6 Knowledgebase Subsystem

This subsystem is responsible for all permanent data storage in the integrated maintenance system and all access controls on that data.

6.1.2.1.7 Logistics Subsystem

This subsystem is the logical representation of a logistics capability in the integrated maintenance system. It is responsible for maintaining and coordinating all transportation and storage needs of the integrated maintenance system.

6.1.2.1.8 New System Planner Interface

This interface is to be used in conjunction with researcher interface to support planners/designers of new systems. This will allow planers access to appropriate maintenance information and provide the integrated maintenance system with future capacity requirements.

6.1.2.1.9 Overwatch Subsystem

This subsystem is responsible for all monitoring the status of both supported operational systems as well as the integrated maintenance system itself. This subsystem includes both passive (push) monitoring as well as active (pull) monitoring. Additionally this subsystem is responsible for alerting appropriate other interfaces/subsystems of events in accordance with operational policy. For example while the control over and use of storage facilities is part of the logistics subsystem; the Overwatch subsystem is responsible for notifying other subsystems when the storage facility reaches a threshold of capacity.

6.1.2.1.10 Operational Site Interface:

This subsystem is responsible for interfacing with operational systems maintained by the integrated maintenance subsystem. Unlike the system owner interface which is intended to interact with the human system owners this interface is to allow automation between (semi-) autonomous systems, the operational system, and the integrated maintenance system. This interface allows an operational system to request a maintenance action, request information about a maintenance action, be notified of certain events in the processing of a maintenance action, as well as inform the maintenance system of its status.

6.1.2.1.11 Repair Depots Subsystem

This is the logical representation of depots in the integrated maintenance system. As the integrated maintenance system is responsible for maintain itself this subsystem is also operational support of the integrated maintenance system itself.

6.1.2.1.12 Reporting Subsystem

This subsystem is responsible for the aggregation and dissemination of all structured data throughout the integrated maintenance system.

6.1.2.1.13 Researcher Interface:

This interface supports researches in performing analysis on operational systems supported by the integrated maintenance system and the integrated maintenance system itself. This is interface will provide data and access restricted by operational policy by interacting with the knowledgebase, reporting, tracking and simulation subsystems.

6.1.2.1.14 Security Subsystem (not shown)

In addition to the physical security measures required at facilities operated by integrated maintenance system additional safeguards providing for Operation Security (OPSEC), Information Security (INFOSEC), Transmission Security (TRANSEC), Communications Security (COMSEC), and Emissions Security (EMSEC or TEMPEST) will be automatically enforced. While not shown in Figure 6.1-2 for readability reasons (the security subsystem interacts with every other subsystem) it is a core component of the system. This subsystem provides for the centralized management of authorization and access controls within the integrated maintenance system. This subsystem also has responsibility for removing information from data aggregation in order to ensure that security safeguards are met.

6.1.2.1.15 Shared Resources Subsystem

This subsystem is responsible for coordinating access to shared resources. This includes both equipment and personnel that are capable of supporting/existing at multiple physical locations or being used by multiple subsystems. For example while the communications subsystem is responsible for actually transmitting data on a communications link it is the shared resources subsystem that is responsible for ensuring that all subsystems have appropriate access to the communications link itself.

6.1.2.1.16 System Owner Interface:

This subsystem is responsible for interfacing with system owners. These include the owners of operational systems supported by the integrated maintenance system as well as the owners of the integrated maintenance system itself. In support of this the interface primarily interacts with the reporting subsystem to provide appropriate information to the system owners as well as to the control system to process any commands from system owners. This subsystem is an active interface capable of initiating interaction (via sending information without an explicit request) as required by operational policy.

6.1.2.1.17 Vendor and Outsourced Maintenance Interfaces

This interface supports the Vendor and Outsourced Maintenance external systems. These interfaces are for access from the integrated maintenance system into the appropriate external maintenance system. This allows the integrated maintenance system to maintain information and visibility (as determined by service level agreements) along the entire maintenance trail. Secondly, this interface provides the ability for the integrated maintenance system to execute "data calls" as determined by operational policy. These data calls may be triggered by an external request or by the integrated maintenance as part of its normal operations (for example in response to a low inventory threshold).

6.1.2.1.18 Workflow Tracking Subsystem

This subsystem is responsible for tracking a maintenance action throughout integrated maintenance system. This subsystem is similar to the Overwatch subsystem but focused on tracking an actions progress/status within the integrated maintenance system.

6.1.3 Maintenance Use Cases

The integrated maintenance system exists to optimize the execution of the maintenance mission for operational systems; therefore, it is necessary to establish baseline use cases of what it means to execute the maintenance mission. The integrated maintenance mission consists of two primary use cases: ad hoc maintenance and scheduled or commanded maintenance. The primary difference between the two maintenance use cases is whether there is advance knowledge, before an incident, that maintenance is required.

6.1.3.1 Ad Hoc Maintenance Use Case

Ad hoc maintenance occurs when an operational system either fails to function or gives a failure indicator. The primary characteristic of ad hoc maintenance is that the triggering event within the operational system is a failure or fault of some sort and therefore, the maintenance action is a reaction to restore the operational system to a fully operational state.

Ad hoc maintenance is an unscheduled maintenance action, often taken by surprise. This unscheduled event could be an expected failure or degradation with unknown occurrence or completely unknown with regard to its operational consequence and timing. There is no planning for a specific ad hoc maintenance action, only capacity planning based on past data, statistical analysis and probabilistic inference. The ability to perform multiple ad hoc maintenance tasks at the same time, where the operational system mimics Murphy's Law by having many operational components breaking simultaneously, is a major reason why most system owners are reluctant to reduce or share their respective maintenance resources.

Figure 6.1-3: Ad Hoc Maintenance in the Integrated Maintenance System Use Case illustrates this particular use case.

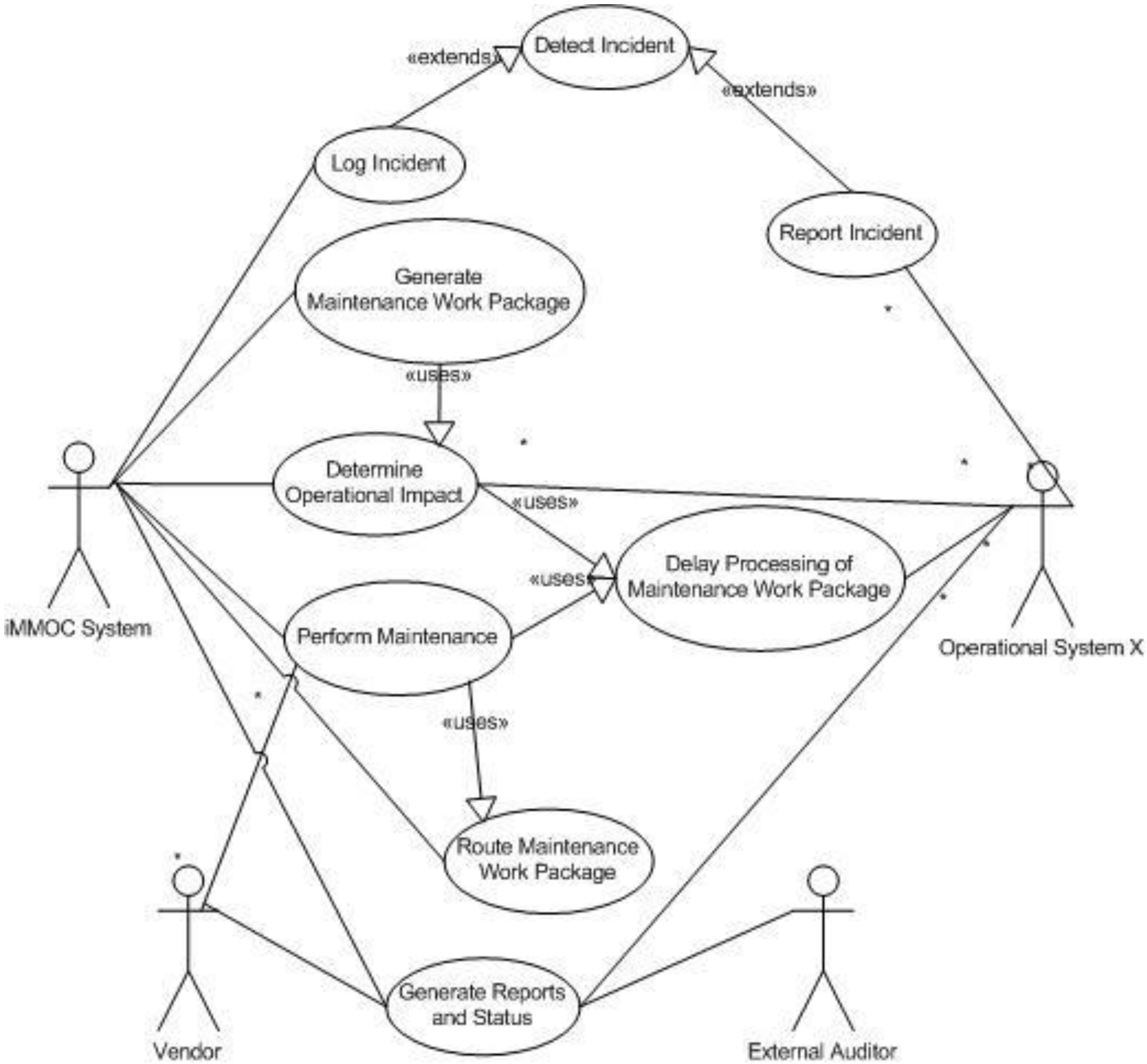


Figure 6.1-3: Ad Hoc Maintenance in the Integrated Maintenance System Use Case

6.1.3.1.1 Ad Hoc Maintenance Use Case Narrative

1. The operational site detects an anomalous condition that requires maintenance action.
2. The operation site determines the overall operational impact to the system
3. The operational site reports the event to the iMMOC
4. The iMMOC records the event's details (description, priority, timestamp, etc) and initiates an ad hoc maintenance request.
5. The iMMOC queries the operational system if the request should be performed immediately or if the request should be delayed to a more opportune time to limit operational impact (for the specific case where the ad hoc maintenance brings the entire

system offline, the operational system owners are given the option to continue in a degraded mode for as long as desired).

6. The operational system either requests maintenance be performed immediately or gives a desired window of opportunity to complete the maintenance action. If the action is intentionally delayed, the ad hoc maintenance changes to a commanded and scheduled maintenance request.
7. The IMMOC determines the responsible maintenance site (back to site, depot, or factory) to which the defect and maintenance work package are to be sent, or the site excesses the equipment requesting a spare, or continues to use the defective part at a degraded capability as deemed appropriate per business policy.
8. The defect and associated work package transit to the responsible maintenance site, entering the integrated maintenance system.
9. The responsible maintenance site attempts repair the defect and execute the work package. If the site cannot execute the work package or if the site is not able repair the defect, then restart at step 7.
10. The repaired or replaced part and completed work package transit back to the requesting site. If the requesting site is not the originating site, then step 8 continues until the work package and part reach the originating site.

6.1.3.2 Commanded and Scheduled Maintenance Use Case

Scheduled and commanded maintenance are types of preventative maintenance. The difference is in the origination of the maintenance request. In scheduled maintenance, the operational site originates the maintenance request based on its own schedule and operational imperatives in order to be compliant with its established maintenance procedures and CONOP. This is different from incident handling and ad hoc maintenance as these maintenance requests are not initiated due to a problem, rather they are initiated as part of the SOP to prevent problems.

Commanded maintenance is similar to the scheduled maintenance except the IMMOC or other external entity directs the operational system to make a change. Therefore, commanded maintenance actions are reported as changes not incidents. Examples of commanded maintenance include directed software upgrades due to licensing or patch compliance issues. Since commanded maintenance results in a change to the operational system rather than a fix, it resets the operational baseline and requires execution of the appropriate change control procedures and updating all relevant operating and maintenance procedures, possibly requiring renegotiation of the maintenance service levels currently in place.

Regardless of whether maintenance is scheduled or commanded, and unlike ad hoc maintenance, there is a priori knowledge that the maintenance action will occur, and therefore, appropriate capacity planning and scheduling can be performed.

Figure 6.1-4: Commanded and Scheduled Maintenance in the Integrated Maintenance System Use Case illustrates this use case.

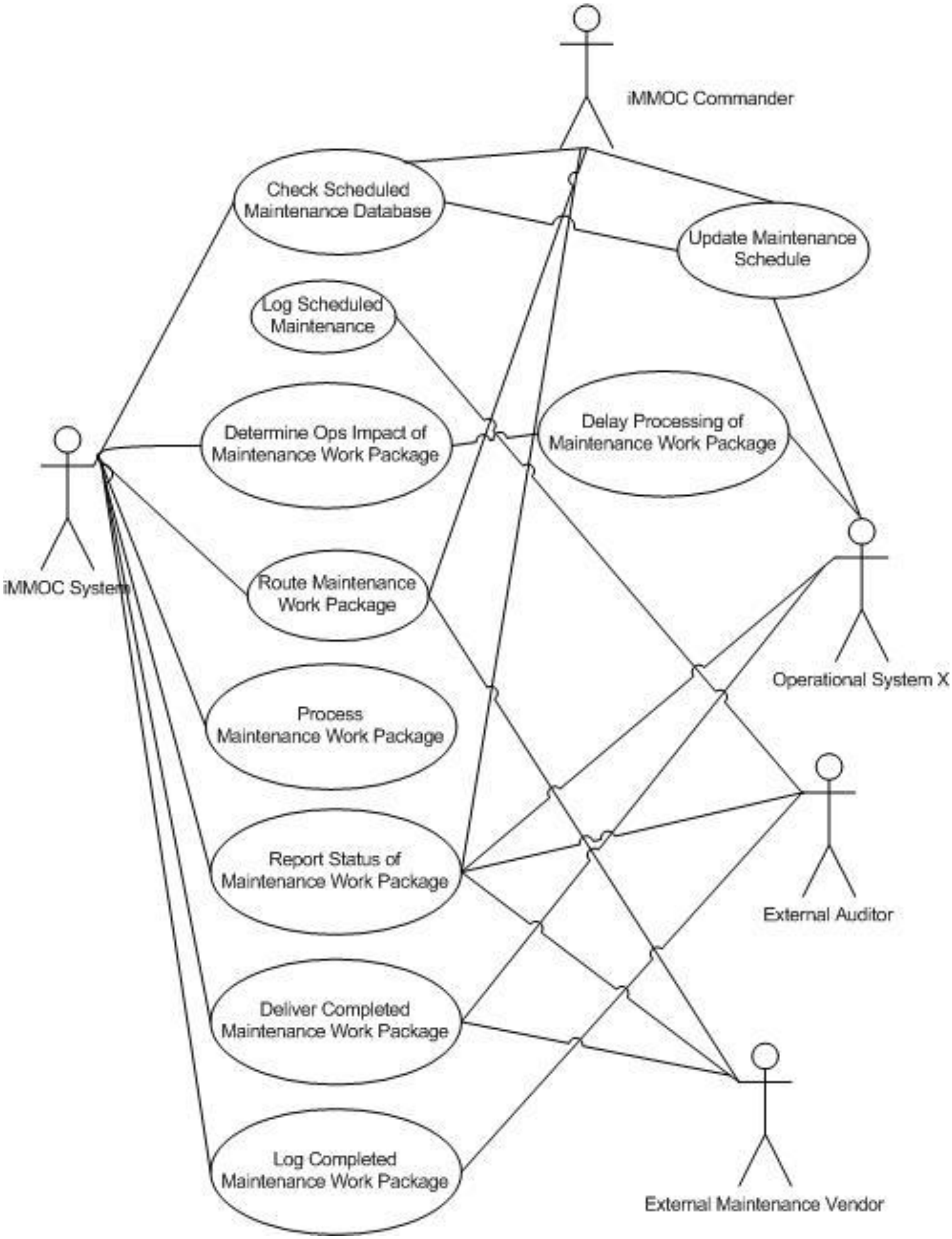

iMMOC Commander
Check Scheduled Maintenance Database
Update Maintenance Schedule
Log Scheduled Maintenance
Determine Ops Impact of Maintenance Work Package
Delay Processing of Maintenance Work Package
iMMOC System
Route Maintenance Work Package
Operational System X
Process Maintenance Work Package
Report Status of Maintenance Work Package
External Auditor
Deliver Completed Maintenance Work Package
Log Completed Maintenance Work Package
External Maintenance Vendor

Figure 6.1-4: Commanded and Scheduled Maintenance in the Integrated Maintenance System Use Case

6.1.3.2.1 Commanded and Scheduled Maintenance Use Case Narrative

1. Change the system (or subsystem/component) state from "operational" to "maintenance"
2. The site makes a request for maintenance and the system determines the responsible maintenance site to which the defect and maintenance work package are to be sent, or the site excesses the equipment requesting a spare, or continues to use the defective part at a degraded capability as deemed appropriate per business policy
3. The defect and associated work package transit to the responsible maintenance site, entering the integrated maintenance system.
4. The responsible maintenance site attempts repair the defect and execute the work package. If the site cannot if not able to be done at the repair facility then restart at step 2
5. The repaired or replaced part and completed work package transit back to the requesting site. If the requesting site is not the originating site, then step 5 continues until the work package and part reach the originating site.
6. Change the system state from “maintenance” to "operational"

6.2 Maintenance System Evolution

The historical maintenance system, prior to integration, consisted of a three-tiered structure, of site, depot, and factory, as illustrated in Figure 6.2-1 (A). However, the generalized form of a three-tiered structure is an n-tiered structure, in which an arbitrary number of nodes can be inserted between the root and leaf nodes.

Figure 6.2-1 (B) shows how the addition of a second depot creates a four-tiered chain. Figure 6.2-1 (C) shows how the two depots (or an arbitrary number of depots) are logically grouped together to pull the chain to three tiers, allowing the three-tiered maintenance structure to be logically extended to n-tiers without changing the perspective of the leaf nodes.

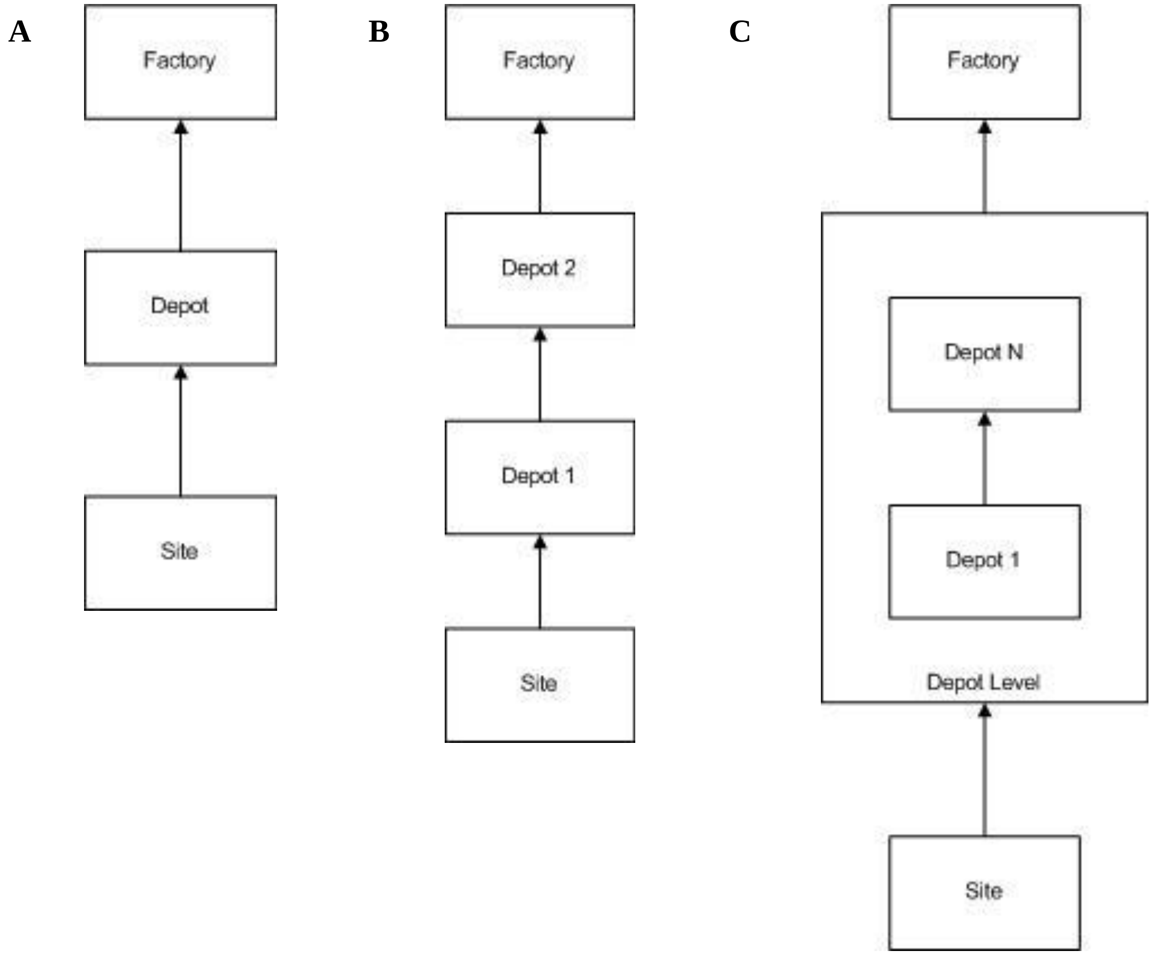


Figure 6.2-1: Integrated Maintenance Evolution to an n-Tiered Chain

Figure 6.2-2 highlights multi-site extensions to the traditional chain consisting of a single depot supporting a single site (Figure 6.2-1 (A)). Multi-site extensions, in which a single depot supports more than one leaf node, as in Figure 6.2-2 (A) or more than one subordinate node, as in Figure 6.2-2 (B) are critical to achieving the sponsor project goal of decreasing the number of maintenance depots required to support operational systems. Figure 6.2-2 (A) shows the logical collapse of a maintenance system in which the depot supporting Site 2 is decommissioned and Depot 1 takes over the support for Site 2. Figure 6.2-2 (B) shows decommissioning of the Factory supporting Depot 1, and the injection of Depot 2 into the maintenance chain for Site 1.

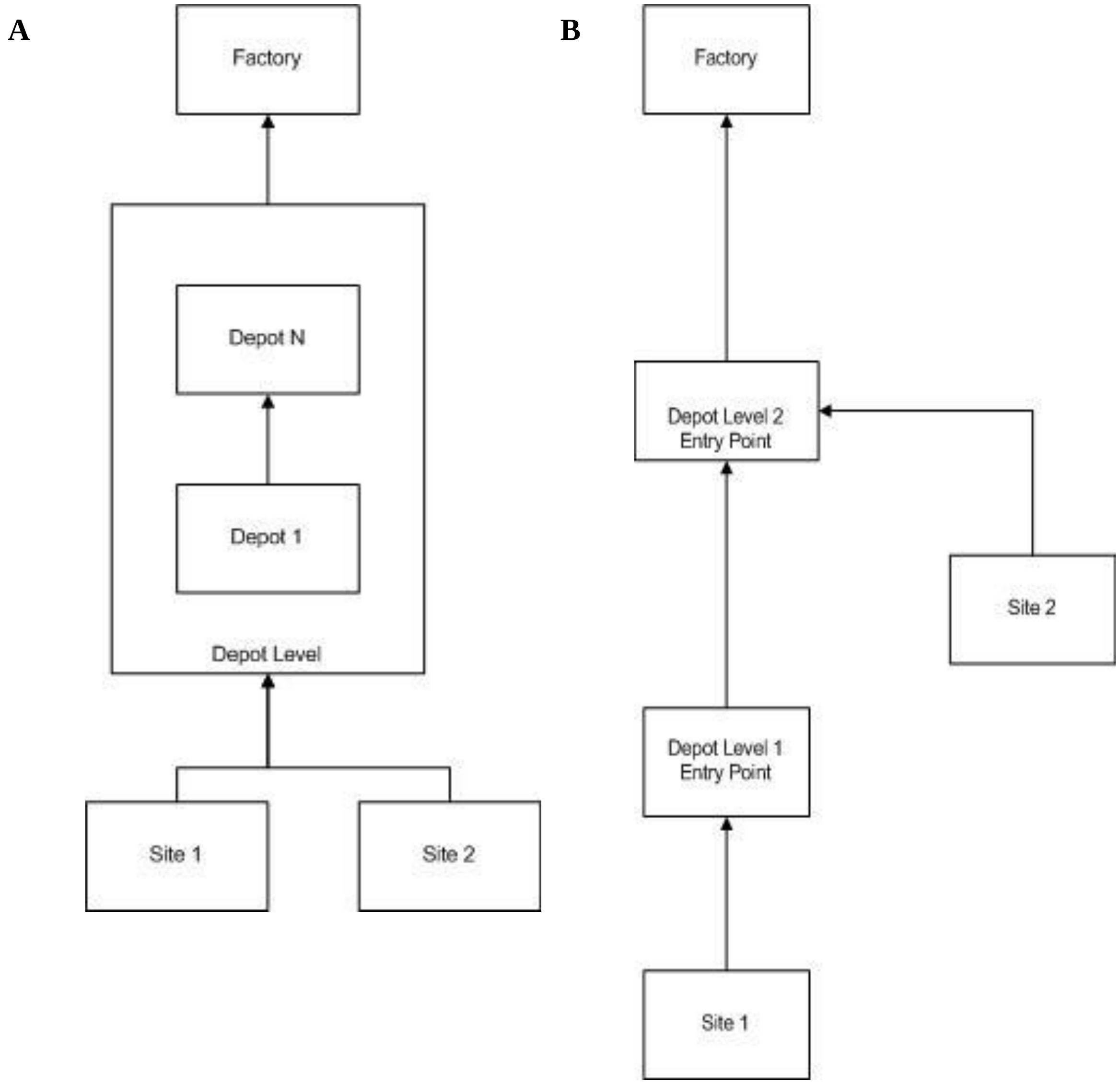


Figure 6.2-2: Multi-Site Extensions to the Integrated Maintenance Chain

Figure 6.2-3 shows the maintenance system evolution from multi-site chains at the depot level to multi-depot chains at the factory level. In addition to multiple depots supported by a given factory, each site can have an arbitrary number of depots situated between it and its supporting factory. Each branch in the maintenance tree is independent of the other branches, and each branch may have an unlimited number of leaf nodes (as indicated in Figure 6.2-2). Implicit in Figure 6.2-3 is the assumption that a given node in the maintenance tree can only escalate, not transfer work. This assumption is graphically represented by the fact that nodes only have vertical paths to parent nodes in common but no horizontal paths to peer nodes.

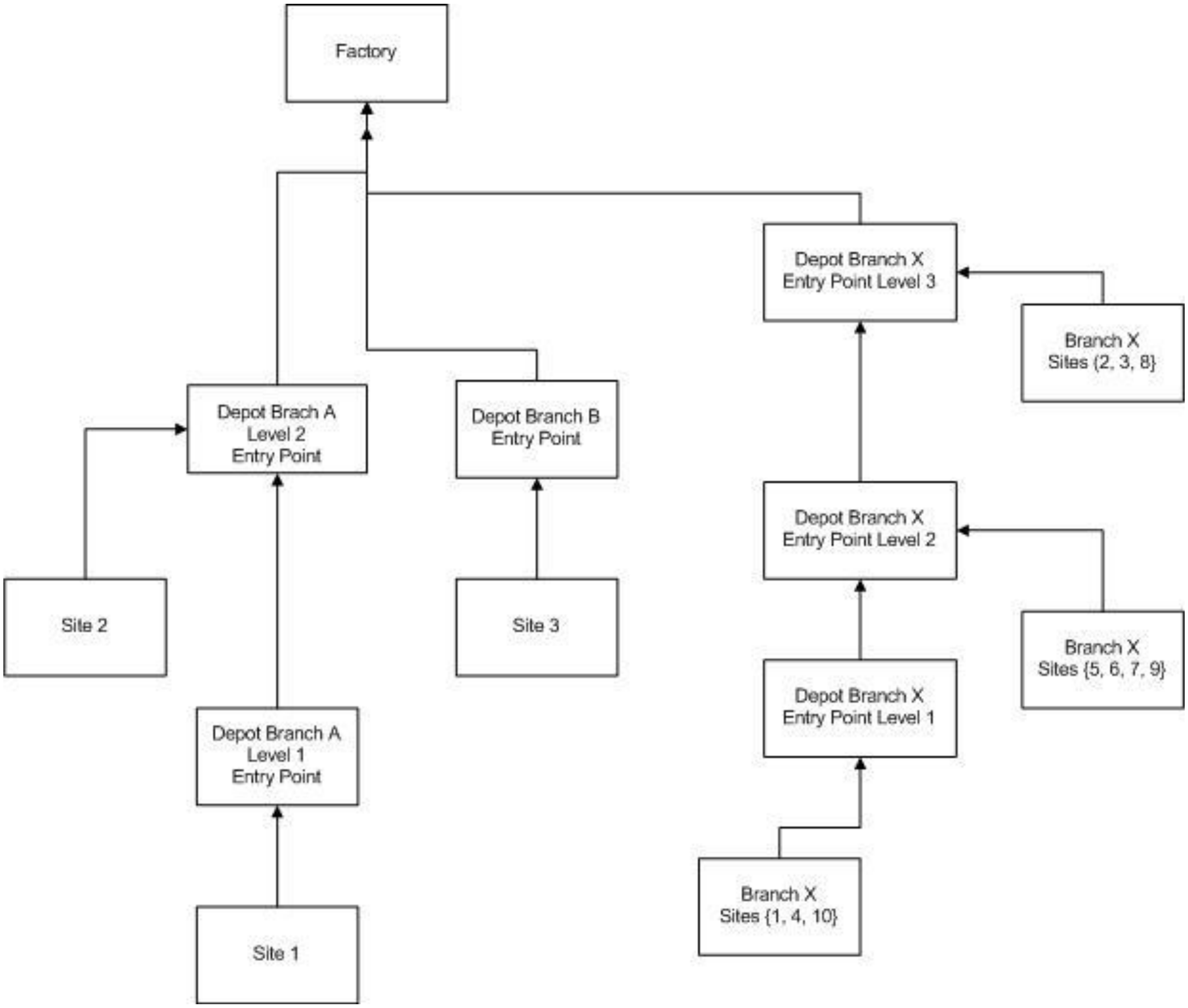

Factory
Depot Branch X Entry Point Level 3
Branch X Sites {2, 3, 8}
Depot Brach A Level 2 Entry Point
Depot Branch B Entry Point
Depot Branch X Entry Point Level 2
Site 2
Site 3
Branch X Sites {5, 6, 7, 9}
Depot Branch X Entry Point Level 1
Depot Branch A Level 1 Entry Point
Branch X Sites {1, 4, 10}
Site 1

Figure 6.2-3: Evolution of Multi-Site Maintenance Chains To Multi-Depot Chains

Figure 6.2-4 highlights the routing issues that Figure 6.2-3 suggests. Examination of the depot level of the maintenance chain in Figure 6.2-4 shows that there are no horizontal work transfers allowed in the tree. Depot 1a cannot shift work to Depot 1b, regardless of whether Depot 1b is capable of executing the work. Figure 6.2-4 (A) shows the scenario in which Depot 1a there is no common parent between Depot 1a and Depot 1b, so work that Depot 1a cannot complete must be escalated to either a higher-level depot or a factory. Work sent to a higher-level echelon is presumed to be at a higher cost because of the increased level of skill implied in higher-level maintenance organizations. Additionally, work escalation due to capacity limits (time, space, personnel, spares) as opposed to work escalated due to specialized requirements only present at the higher echelon risks of disrupting other work currently under way at the higher echelon maintenance organization.

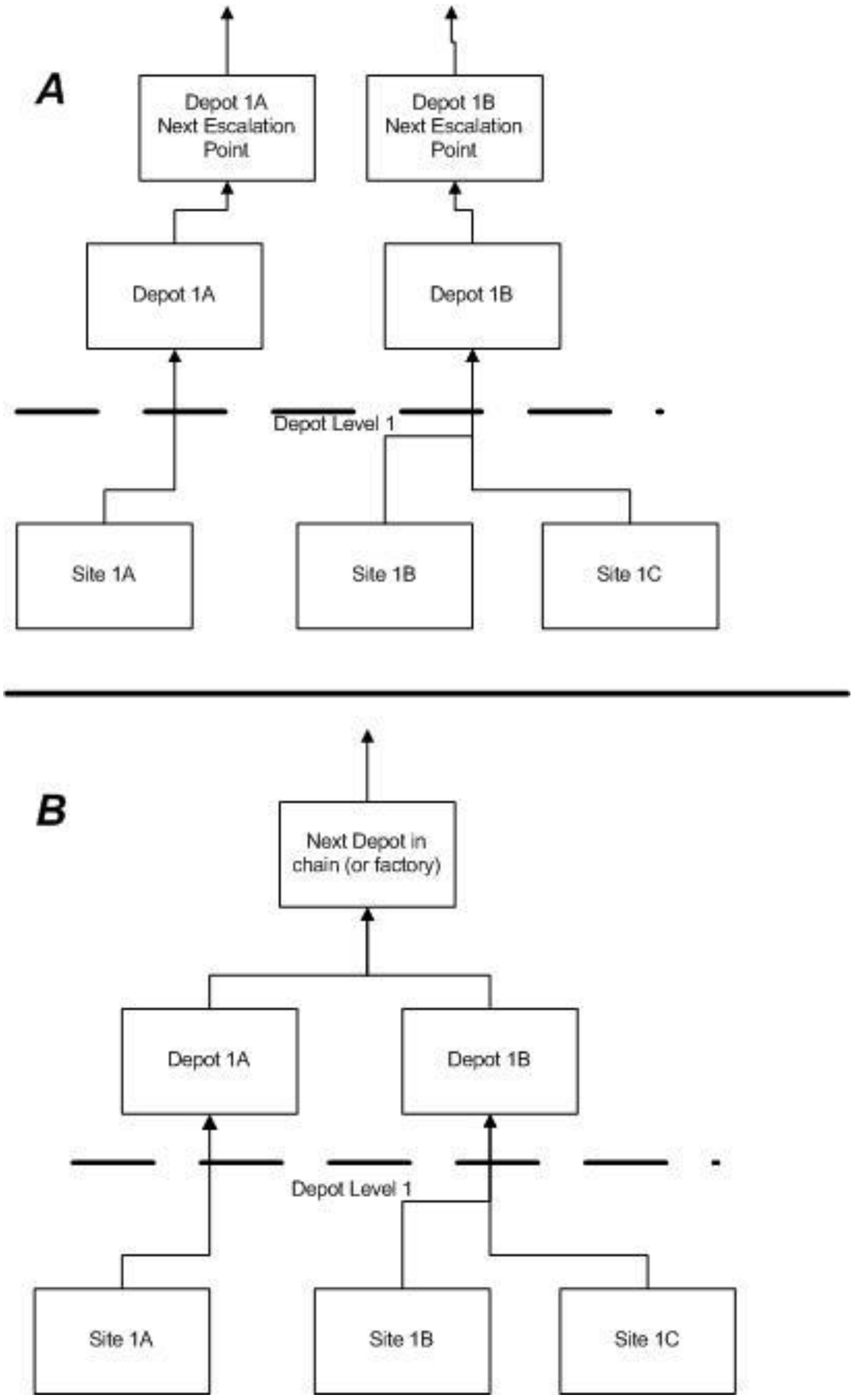


Figure 6.2-4: Lack of Centralized Control Prohibits Horizontal Work Shifts and Mandates Escalation

Figure 6.2-4 (B) extends Figure 6.2-4 (A) by putting place a common parent between Depot 1a and Depot 1b. In this scenario, the higher-echelon depot can accept the work from Depot 1a and reroute the work to Depot 1b, which upon completion must route the work back to the parent depot, which will then reroute it to Depot 1a. Depot 1a will not be aware that Depot 1b executed the maintenance task, because it sent the work to the parent depot. Similarly, Depot 1b will not be aware that Depot 1a requested the work, as it was assigned the task by its parent depot. While this is good information hiding, it is a waste of time as the parent depot does not perform value-added work and a waste of time, as the work requested may actually require the shipment of physical goods from Depot 1a to the parent to Depot 1b and back.

As in Figure 6.2-4 (A), the time spent transshipping work from Depot 1a to the higher-echelon depot to Depot 1b and back equates to cost and risk.

Figure 6.2-5 continues the evolution of the integrated maintenance concept by focusing on Command and Control integration into the maintenance graph. Specifically, the introduction of IMMOC initiated Command and Control functions allows for the horizontal transfer of work between peers, regardless of where (or if) there is a parent node in common between the nodes. Execution of a horizontal transfer requires the establishment of ad hoc links between the nodes for the purpose of work transfer and return transfer. The costs of the transfer must be factored in to the decision to execute an ad hoc horizontal transfer over a pre-planned escalation. However, these costs should, in general, be equivalent for logical transfers as the costs of network bandwidth are shared across the system. For physical transfers the costs would presumably be less than a series of escalations to a common parent as there are only two physical transfers (Depot 1a to Depot 1b and back) as opposed to the four transfers required in Figure 6.2-4 (B).

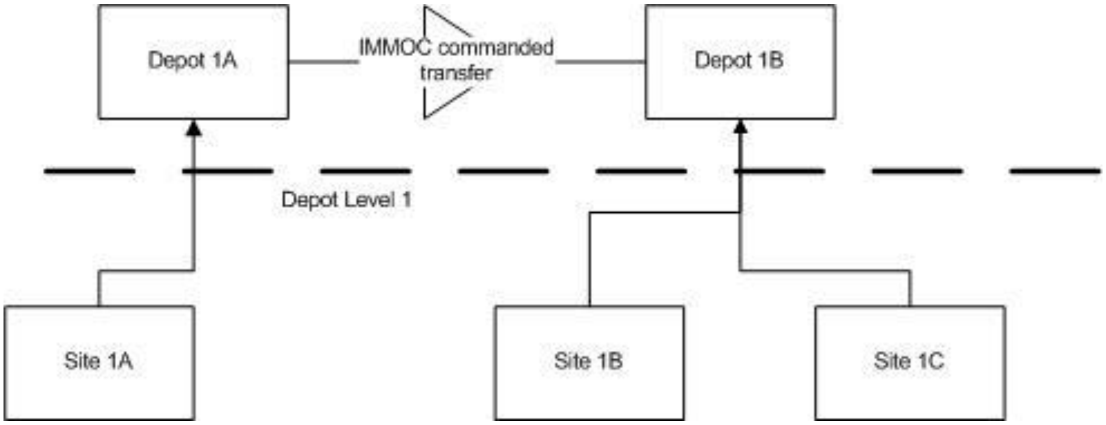


Figure 6.2-5: IMMOC-Directed Maintenance Action Rerouting

The issue of costs shows that the IMMOC must consider a series of constraints before issuing a horizontal transfer command. The constraints that are factored into the optimization problem include the costs of escalation vs. horizontal transfer in time and dollars, the risk of work interruption, security handling, information sharing risks, and capacity throughout the system.

Figure 6.2-6 shows the ultimate evolution of the integrated maintenance system into a forest, with multiple factories as the root nodes of each tree in the forest. The IMMOC performs Command and Control functions, directing traffic throughout each tree, and most importantly, allowing the dynamic rerouting of traffic between levels within a tree on an ad hoc basis or even between trees in the forest.

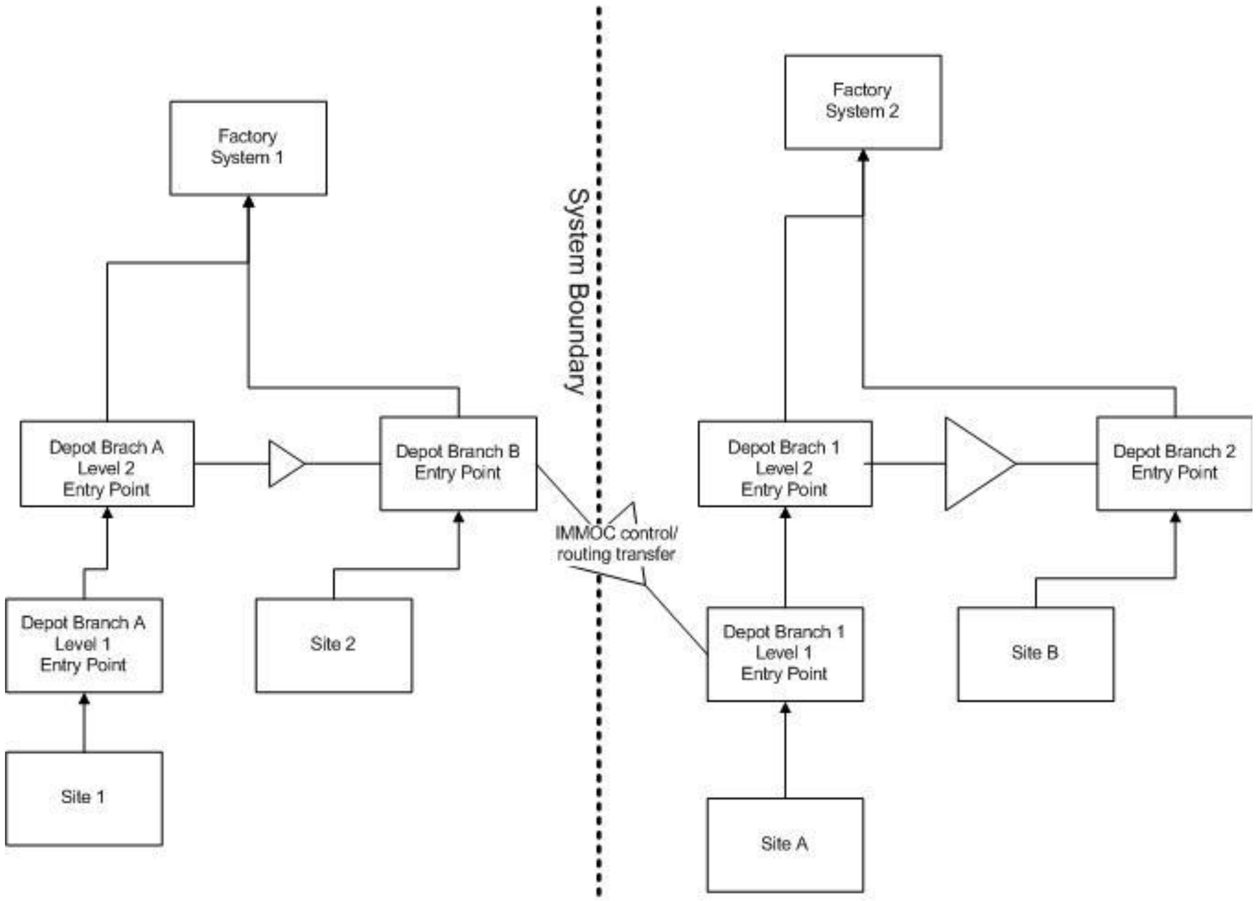

Factory System 1
Factory System 2
System Boundary
Depot Brach A Level 2 Entry Point
Depot Branch B Entry Point
Depot Brach 1 Level 2 Entry Point
Depot Branch 2 Entry Point
IMMOC control/ routing transfer
Depot Branch A Level 1 Entry Point
Site 2
Depot Branch 1 Level 1 Entry Point
Site B
Site 1
Site A

Figure 6.2-6: IMMOC Command and Control Across the Maintenance System

Routing decisions are made to optimize overall system performance and routing commands ensure traceability for maintenance execution as well as cost accounting purposes.

6.3 Integrated Maintenance System Behavior

The primary mission of any maintenance system is to maximize the operational use of the systems it maintains. Traditionally this has meant optimizing the maintenance paths that various sub assemblies require. While this capability is still present in the integrated maintenance system an additional Command and Control capability is present that allows for analysis and optimization at a system rather than subassembly level.

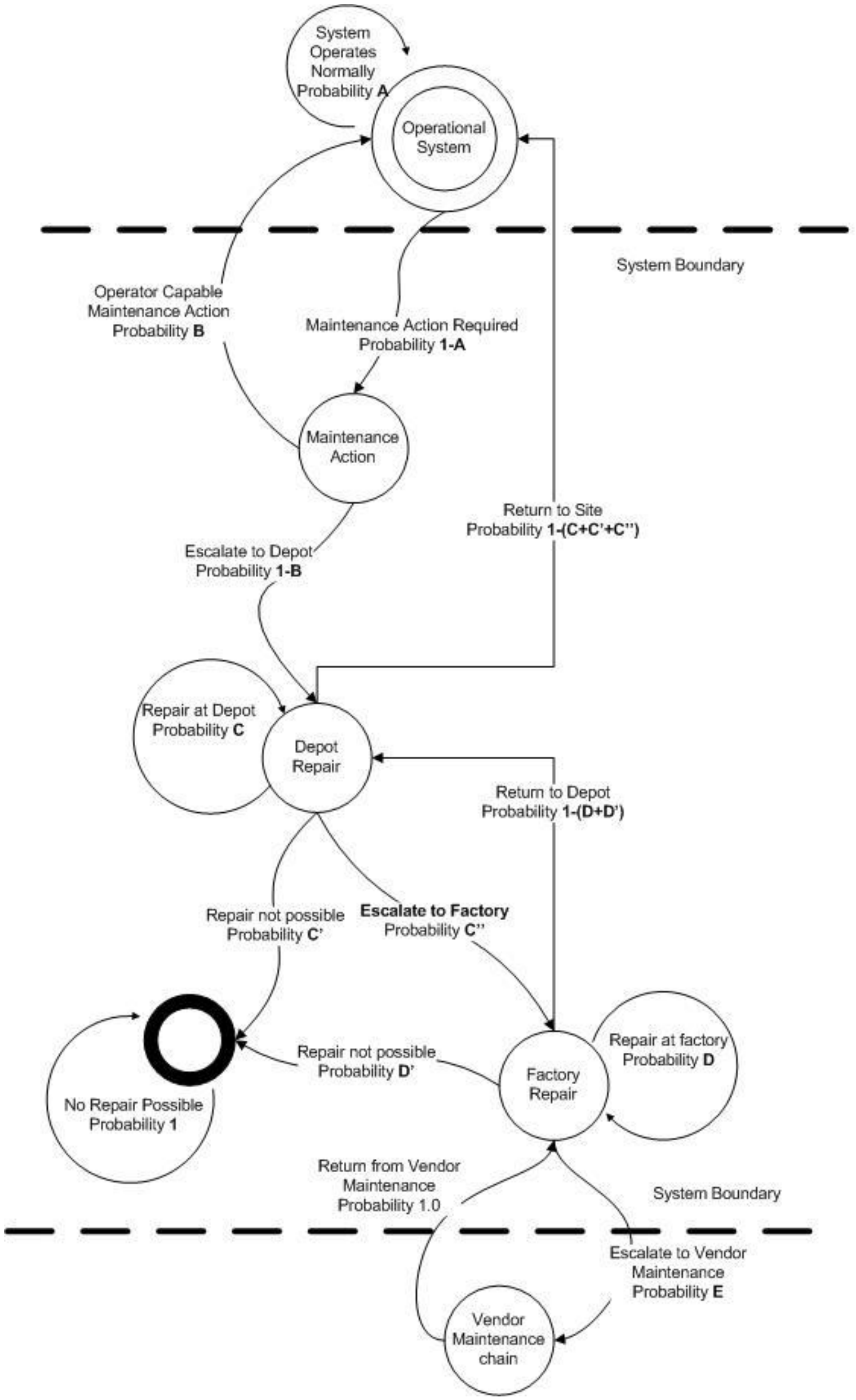

System Operates Normally Probability A
Operational System
System Boundary
Operator Capable Maintenance Action Probability B
Maintenance Action Required Probability 1-A
Maintenance Action
Return to Site Probability 1-(C+C'+C")
Escalate to Depot Probability 1-B
Repair at Depot Probability C
Depot Repair
Return to Depot Probability 1-(D+D')
Repair not possible Probability C'
Escalate to Factory Probability C"
Repair at factory Probability D
Repair not possible Probability D'
Factory Repair
No Repair Possible Probability 1
Return from Vendor Maintenance Probability 1.0
System Boundary
Escalate to Vendor Maintenance Probability E
Vendor Maintenance chain

Figure 6.3-1: Maintenance System State Transition Diagram and Markov Chain – Subassembly Point of View

6.3.1 Traditional Subassembly Repair

In a traditional maintenance model, subassemblies are repaired as needed. This repair may be an actual repair to the component or a replacement with a spare from inventory. The focus is on returning the system to its original state without modification. At each stage of the repair cycle (site, depot, and factory) an analysis can be done to determine what the potential benefits are of allocating additional resources to that state to lower the probability of requiring escalation to complete the repair. While this could provide for future cost savings and efficiencies in repair times, it does not provide any benefit to the operational system at the current point in time. This is because the focus on this chain of events is on the execution of the repair instead of on maintaining a system in an operational state. To achieve this goal the integrated maintenance system provides a second top-level state model, as illustrated in Figure 6.3-1: Maintenance System State Transition Diagram and Markov Chain, to provide the Command and Control capability necessary to maximize operational system uptime.

6.3.2 Maintaining Operational Capability

This second state diagram, Figure 6.3-2: Maintenance System State Transition Diagram – IMMOC Point of View, is superimposed upon the traditional repair states by the Overwatch and Command and Control subsystems of the integrated maintenance system. The focus of this state chain is to provide the ability to control repairs so that the operational system is available to perform its mission as required. Additionally this aggregation of repair activities allows the system owners a greater level of optimization. It is now possible to optimize across subassembly repairs and make resource tradeoffs against operational system availability and levels of degraded capability instead of on single subassembly repair chains. This can take the form of commanding maintenance to coordinate with other systems, baseline changes that have affect multiple subassemblies, as well as decisions to return an operational system to a degraded state from a non-operational state due to that systems mission requirements.

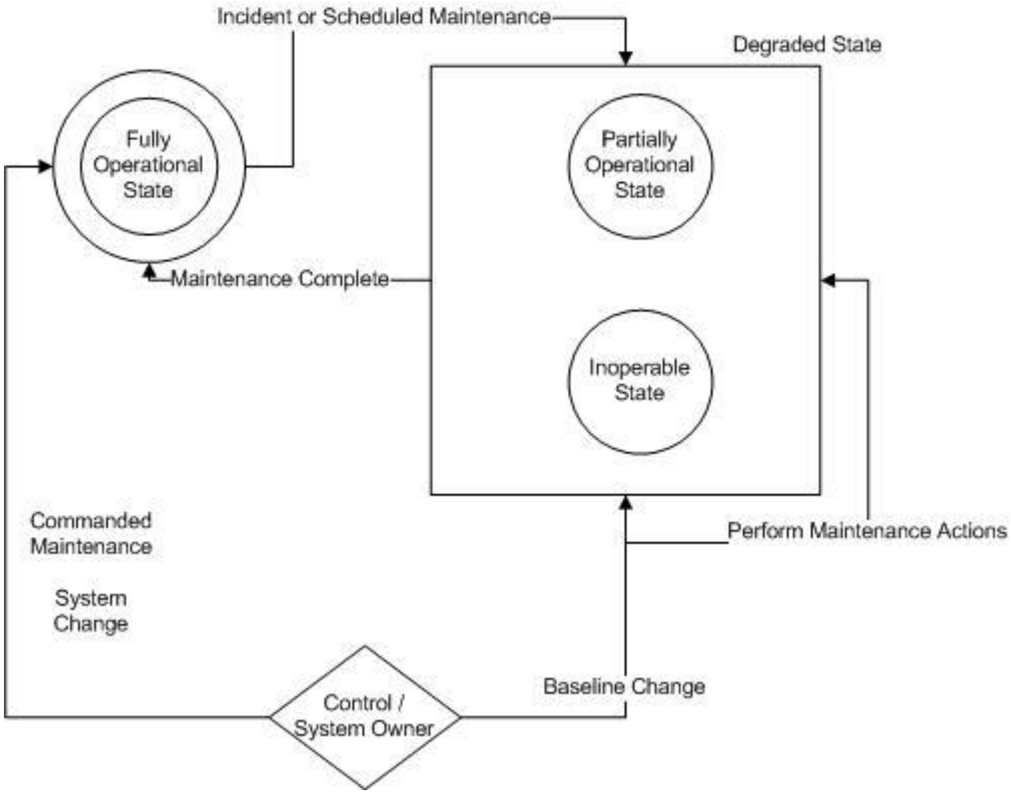


Figure 6.3-2: Maintenance System State Transition Diagram – IMMOC Point of View

6.4 System Optimization

System optimization requires the collection and analysis of metrics, as identified in Section 4.4, Quantitative Measures.

6.4.1 Metrics Collection Drives Behavior Rather than Behavior Driving Metrics

Metrics are a valuable measure of system performance in that they allow quantitative and objective measures of specific events. However, while the measurement of the metric is neutral, the metric itself is not neutral. Metrics immediately create an optimization equation for that part of the system being measured. Namely, for a set of more is better metrics $M \equiv \{M_1, M_1, \cdots, M_n\}$ and a set of less is better metrics $m \equiv \{m_1, m_2, \cdots, m_n\}$, then the system will adjust its behavior to optimize the value of each element of *M* and *m*, that is, the system and its operators will adjust behavior to obtain $\max\left(\sum_1^n M_j\right)$ and $\min\left(\sum_1^n m_j\right)$.

However, in aggregate, $\max\left(\sum_1^n M_j\right)$ and min $(\sum_1^n m_j)$ may not represent optimal behavior. Instead, careful weighting needs to be assigned to each M_j and m_j to ensure that the max and min functions, when optimized, result in optimal system behavior. Typically, harder to achieve or more important metrics carry higher weights than easy to achieve metrics, thereby encouraging behaviors to optimize the higher weighted metrics.

6.4.2 Metrics Collection and Behavior

Additionally, care must be taken when measuring system performance with metrics that represent static averages. For instance, if an average has been collected over a series of years, then the addition of an outlying measure that is three or more standard deviations from the mean may not move the mean due to the calculation of the average. Further, averages hide system behaviors. For instance, if two repairs are executed, whether it takes 10 hours for each repair, or 10 minutes for the first repair and 19 hours and 50 minutes for the second repair, mean time to repair is the same – 10 hours. One way to address this is to collect a moving mean, in which the mean is calculated over the last *n* samples, where *n* is selected to represent some operationally significant unit of time. A second way is to collect additional detail allowing the calculation of metadata around the metric to enable trend analysis, like standard deviation.

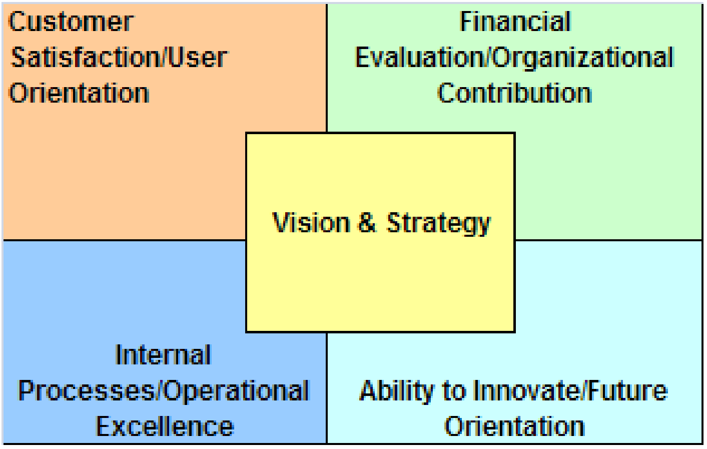

Customer Satisfaction/User Orientation
Financial Evaluation/Organizational Contribution
Vision & Strategy
Internal Processes/Operational Excellence
Ability to Innovate/Future Orientation

Figure 6.4-1: Balanced Scorecard Overview

As with any measurement, care must be taken to ensure that metrics gathered are not only measurable, but that the measurements serve as a proxy for desired system behavior. Gartner Group and other industry researchers recommend applying the balanced scorecard approach to metrics collection. The balanced scorecard concept, highlighted in Figure 6.4-1, shows how vision and strategy (mission execution in the context of this study) are decomposed into four areas. Each of the areas can be independently measured but it is the overall collection of metrics that must be optimized for the Vision and Strategy mission to be fully realized..

6.4.3 ITIL Metrics Mapped to an Operational Balanced Score Card

In conjunction with Figure 6.4-1, Table C-1: Key Considerations in Metric Collection for Maintenance Systems, maps common metrics, as defined by ITIL, Gartner Group, and Burton Group, to each of the balanced scorecard quadrants, as identified in Figure 6.4-1.

7.0 Conclusions

The analysis executed to deconstruct the problem associated with creating an integrated maintenance system by extracting organic maintenance segments from operational systems such as AEHF, DMSP, DSP, GSP, SBIRS, and TSAT resulted in numerous conclusions, some of which were neither surprising nor new:

- CMMI and ITIL are directly applicable to all aspects of the maintenance mission not just the IT aspects
- The Command and Control mission is dependent on and more valuable than the Overwatch mission
- Numerous optimization points exist with regard to system resources and optimal system design is non trivial
- Standardized metric definitions are required in order to evaluate integrated maintenance mission effectiveness

However, three conclusions were unexpected:

- Numerous synergies exist that can potentially offset the implementation costs of the integrated maintenance mission system beyond traditional consolidation savings.
- Aggregated data and standardized metrics enable the generation of a class of metrics targeted specifically at maintenance execution.
- The a priori conclusion that COTS and GOTS components are cheaper than custom components does not hold when looked across the entire system lifecycle

Listed in alphabetical order, the seven most significant conclusions resulting from the mission analysis, functional decomposition, and requirements analysis are identified below.

7.1 Applicability of ITIL and CMMI to Integrated Maintenance Operations

As the study progressed, it became rather clear that successful implementation of an iMMOC concept is highly dependent upon the proper adaptation of Information Technology Infrastructure Library (ITIL) and Capability Maturity Model Integration best practices. ITIL is a collection of best practices designed to help manage IT services but can be abstracted to apply more generally to any service of which information is the key component. The integrated maintenance system benefits from this as the information about the maintenance actions not the physical activity is the new component being managed and provided. CMMi best practices are designed to ensure that information and procedures become institutionalized and continually improve over the lifetime of an organization. Together these libraries provide the building blocks for a continually improving both the quality and reliability of the services the integrated maintenance system offers as well as reducing the cost for those services.

The following is a brief extraction of some of the most directly applicable ITIL and CMMi concepts and best practices. This list is by no means exhaustive and serves to demonstrate that the service oriented nature of ITIL and CMMi are readily adaptable to the integrated maintenance system. The major ITIL processes and their applicability to the IMMOC are:

Figure 7.1-1: ITIL Processes Feed the IMMOC Design

- Mapping of the iMMOC principle management functions, specifically
- Incident and Problem Management Lifecycle (to include critical metrics)
- Performance Management (to provide appropriate meaningful metrics)
- Demand Management (to provide proper resource allocation and escalation policies)
- Multiple ITIL modeling techniques (to provide data centric, logistic centric, and workflow centric optimization strategies)
- Incident and Problem Management Data Flows (to ensure that information is routed to those that need it)
- Capacity Management Activities Planning and Execution (to ensure that future needs can be met)

Ultimately, ITIL and CMMI represent a best of breed approach to maintenance as a service – well-documented, repeatable, quantitatively measured, and incrementally improved and optimized processes. However, while CMMI describes how to create the processes and what the processes should address and ITIL documents IT specific processes, the physical aspects of maintenance need to be addressed. The IT aspects of the integrated maintenance system easily support ITIL, however each of the IT processes requires an analogous process for the physical environment in which the integrated maintenance system will operate. The overall creation of the physical analogues to the ITIL processes may enhance their virtual applicability as well. For example, Capacity Planning has a physical dimension, whether for network capacity or manufacturing capacity. In the former, physical dimensions take the form of HVAC, space, and power for network gear instead of workers and manufacturing tools.

7.2 Command and Control vs. Overwatch

The study highlights two primary missions for which the iMMOC would be responsible. The first, identified as Overwatch, performs the function of monitoring the status of all integrated maintenance assets that are tied to the iMMOC system. The primary focus of Overwatch is to collect all pertinent maintenance data (e.g., metrics, and trends) and then report it to operational stakeholders for purposes such as capacity planning and demand forecasting. Although the data to be collected is extensive and important, this Overwatch mission is rather limited in impact by only providing stakeholders insight in the form of status reports. In the context of the iMMOC, stakeholders are able to see where efficiencies may lie within the system but are unable to command or control changes within the iMMOC that enable those efficiencies be realized.

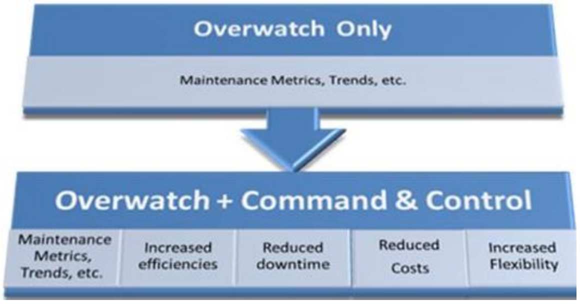

Overwatch Only
Maintenance Metrics, Trends, etc.
Overwatch + Command & Control
Maintenance Metrics, Trends, etc.
Increased efficiencies
Reduced downtime
Reduced Costs
Increased Flexibility

Figure 7.2-1: Command and Control Mission adds significant capability to iMMOC

The Command and Control mission, on the other hand, adds a great deal of functionality to the iMMOC in general, as illustrated in Figure 7.2-1: Command and Control Mission adds significant capability to iMMOC. Taking the maintenance data collected in the Overwatch mission, iMMOC users can actually implement a change or improvement through Command and Control commands within the iMMOC system. As stated upfront, the key drivers for moving to an iMMOC-like concept for handling maintenance in similar systems is to realize increased efficiencies, reduced system downtime, and reduce the costs of maintenance. By incorporating a Command and Control mission into the iMMOC, these goals can be achieved through the direct influence of Command and Control capabilities such as capacity management, demand management, and optimization modeling. Additionally, one of other goals is to ensure that consolidating all maintenance activities into an iMMOC system will not result in degraded system performance. In order to gain acceptance for an iMMOC amongst the user community, this caveat simply cannot be ignored. The service routing capability of Command and Control allows ad-hoc or non-default paths to be initiated that provide maximum maintenance capability to high priority systems or unique situations, and ultimately, reduces the likelihood of degraded system performance.

Incorporation of a Command and Control capability is critical to the success of an iMMOC concept. Without it, the iMMOC can only report maintenance status via the Overwatch mission to the various system stakeholders. Many of the maintenance efficiencies that could be achieved from the iMMOC concept will be very difficult to realize if a Command and Control mission is not designed into the iMMOC system. Command and control would be left to each individual system owner---virtually no different from how maintenance is managed currently. Furthermore, the overall maintenance system performance could suffer, as there would be no direct commanding or controlling means to allow iMMOC users to influence the overall management/flow of maintenance activities. There absolutely must be a capability for the iMMOC to reallocate resources on the fly to meet the highest priority needs at any given moment. In essence, this allows the iMMOC to best adapt to real-time events and control the constrained pool of resources in the best manner possible.

7.3 COTS and GOTS Vendors in the Integrated Maintenance System

The cost of COTS and GOTS in the system lifecycle is an ongoing research subject.[19] However, it is usually assumed that the introduction of COTS or GOTS into a system reduces system lifecycle costs.[20]

In exploring the evolution of the integrated maintenance system in Section 6.2, *Maintenance System Evolution*, the team identified a material weakness in the use of COTS or GOTS relative to custom development. Figure 6.2-6: IMMOC Command and Control Across the Maintenance

[19] See, for example, http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/7416/20153/00931307.pdf or www.sei.cmu.edu/programs/acquisition-support/conf/2003-presentations/looney.pdf
[20] See, for example, http://www.military-information-technology.com/article.cfm?DocID=760

System shows that the IMMOC can direct a maintenance action to leave its default maintenance chain and execute within a different maintenance chain. Normally, this action is thought to occur primarily in response to either a disaster recovery scenario or a load-balancing scenario.

There is, however, a common situation in which the IMMOC, or any maintenance system, will direct the handoff of a maintenance action to an ***outside*** maintenance chain (as illustrated in Figure 7.3-1 shows) – that is, a chain that does not necessarily provide either visibility or responsiveness to direction to the maintenance requester. The common scenario is that of repairing COTS or GOTS. In either case, the COTS or GOTS maintenance system must turn over the COTS or GOTS component to the manufacturer for warranty purposes at which point it leaves the integrated maintenance system, and which forces maintenance actions into a wait state pending resolution.

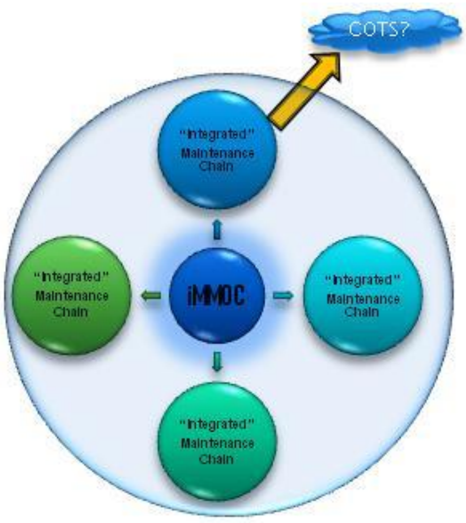

COTS?
"Integrated" Maintenance Chain
"Integrated" Maintenance Chain
iMMOC
"Integrated" Maintenance Chain
"Integrated" Maintenance Chain

Figure 7.3-1: COTS Maintenance Requires External Handoffs

COTS and GOTS hardware presents the least trouble from this perspective, in that if a hardware component is acquired that meets functional and physical requirements and subsequently fails, a new component may be acquired to repair the defective component. However, many modern electronic boards contain not only circuit traces, but often firmware as well. Therefore, when hardware components are returned by COTS and GOTS vendors, it is imperative that not only does the form, fit, and function match that of the defective part, but all the microcode and firmware therein matches as well, else regression testing is required. Since the provider is usually not under obligation to maintain old components (the source of development lifecycle savings), usually a component identical in form and fit and ***primary*** function is returned. If the new hardware requires device driver updates or other software updates, it is the responsibility of the maintenance system to acquire and test these additional components and for the operational system to schedule a change to the system baseline. The key point is that what should have been a simple replacement of a commodity component has resulted in a formal change to the system baseline, driving cost and inducing risk.

COTS and GOTS software presents even higher risk than does hardware. If a hardware component breaks, a new and identical component can be used to replace the defective component, restoring functionality. In software, this is not the case. If a COTS database package is defective, then no amount of swapping it for identical COTS database packages will restore functionality. The vendor must patch the bug. However, since the vendor serves a market that may be vastly large than even that represented by the integrated maintenance system, the operational systems are at the mercy of the COTS software vendor as to the timeliness of any repair. Further, it may be that the COTS or GOTS package under consideration, although perfectly well suited for the mission and the operational system, has been declared obsolete by the vendor and is in an end-of-life state in which no corrective maintenance will be performed by the vendor. Instead, customers must upgrade to a newer, supported version. This scenario, which happens frequently, forces the maintenance system to acquire new licenses, as software upgrades are usually not free to customers. Further, as with hardware, new versions of software require execution of a formal change management process to enable a baseline change. The change process drives costs upwards as regression testing and training are required, and potentially, software and hardware adjacent to the replaced COTS or GOTS software component will have to be modified to accommodate the new software interfaces. This increases risks and costs associated with the maintenance action.

COTS and GOTS hardware do save acquisition costs during development as they spread development costs across the entire customer base of the vendor in question. However, because the vendor serves a larger market than any one customer, more and more often COTS and GOTS products drive interface requirements, leaving systems at risk of significant interface changes during operation as COTS and GOTS components are upgraded during maintenance.

Therefore, while it may be necessary to use COTS and GOTS components, and examination of the maintenance lifecycle of complex systems indicates that COTS and GOTS components need to be carefully constrained within the operational system, preferably through the use of well-defined standards (physical or logical) so as to minimize the risk of interface change and complete regression testing due to a new component matching form, fit, and function, but having changes to microcode, new features not present in the original, or the removal of features considered deprecated by the vendor.

7.4 *Optimization Points*

In any large system, there are multiple points for optimization. A bottom up approach to optimization would focus on the end points, the sites and depots, and how to optimize the effectiveness of each particular node. However, bottom up optimization results in sub optimization across the entire system, as the top level Measures Of Effectiveness (MOE) cannot be optimized by focusing on the bottom level of the system. Therefore, a top down approach must be taken to optimize the system. There are three types of optimization(Figure 7.4-1) that can occur – cost, performance, and schedule. As the cost and schedule dimensions of implementing and operating the integrated maintenance system are beyond the scope of this study, the optimization points discussed herein focus on performance areas that would be worthy of investigation to determine appropriate MOE measures.

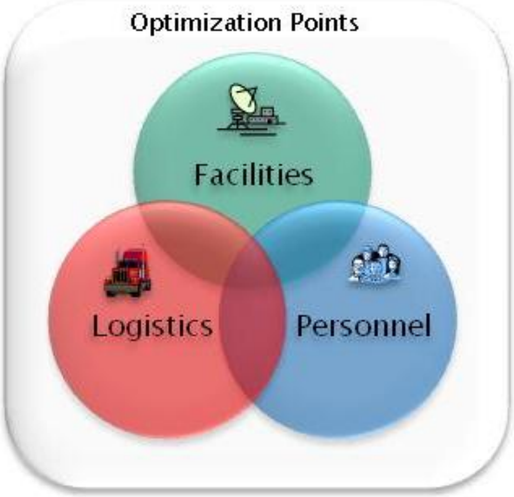


Figure 7.4-1: Facilities, Logistics, and Personnel Represent Major Integrated Maintenance System Optimization Points

7.4.1 *Facilities*

Physical facilities present two obvious points of optimization. The first point is the number of facilities within the integrated maintenance system. More facilities enable greater throughput of parallel tasks, greater distribution of work to facilitate disaster recovery and continuity of operations, smaller drain on local resources (power and water resources are less for small facilities), more diversity in the workforce, fewer disruptions to existing facilities and the potential to facilitate political approval as jobs remain in districts. However, each facility drives cost. Each facility has to have utilities, core physical plant staff, land, transportation, communications, tools, and staff.

The quantity of facilities and their locations represents a traditional integer optimization problem in which there are minimum and target throughput requirements based on a stochastic model for problem occurrence (historical maintenance can be used to generate this function). Models are needed for calculating costs associated with building and maintaining logistics, communications, physical plant, and staffing structures, and stochastic models for mean time to repair based on transportation time.

The facility optimization problem abstracts issues associated with facility fit out – which tool sets are located where. Further, facility optimization should be done with numerous weightings given to existing system locations, as the integrated maintenance system will outlast any given operational system and there is no guarantee that the system locations today will be similar to those chosen tomorrow. Additionally, the optimization problem must take into account restrictions on site locations due to hazardous or oversized cargo.

7.4.2 Logistics

Logistics optimization feeds the facilities optimization problem. Logistics optimization attempts to optimize numerous factors associated with the transportation and communication elements of the integrated maintenance system. Optimization must address cost of service, class of service, make vs. buy for transportation (e.g., outsource to UPS or FedEx vs. building an organic transportation system), limitations on the transportation of hazardous and oversized cargo, security restrictions, and availability of transportation infrastructure.

In addition to transportation issues, logistics optimization must also take into account time to transport material from site to site.

Communications optimization needs to address issues with bandwidth, latency, and network topology as a function of cost. Currently, communications optimization is the subject of much study as converged voice, video, and data services, coupled with new wireless services and presence information enables bundling of services not previously available and the transfer from telecommunications switches to server-based infrastructure.

Logistics optimization is a growing area of research[21].

7.4.3 Personnel

Personnel and workforce optimization is a critical issue facing every organization, public or private. For instance, the United States military invests heavily in operations research[22] to help model the appropriate size and composition of the future force. Personnel optimization accounts for not only the costs associated with the workforce – hiring, training, retaining, salary, and benefits – but also the size and skill mix.

All personnel factors are directly affected by worksite location.

[21] http://cougaar.org – COUGAAR, the Cognitive Agent Architecture, is an open source implementation of the Defense Advanced Research Project Agency research into agent-based logistics modeling.

[22] The United States Navy sponsored a multi-million dollar development effort called COMPASS – Comprehensive Optimal Manpower and Personnel Analytic Support System.

7.5 Standard Metric Definitions and Maintenance-Oriented Metrics

Quantitative measurement is essential to any successful process improvement activity and lifecycle cost assessment. Quantitative measurements, in the form of metrics, form the objective basis for formulating conclusions, performing trend analysis, and performing capacity and demand planning. While the value of metrics as a management and forecasting tool has not been a subject of debate, there is considerable debate, outside of "core" metrics identified in Appendix B, Key Operational Metrics, as to which metrics to gather. Further, there is debate as to the utility of the core operational metrics to the execution of maintenance tasks, as the metrics predominantly address operational, rather than maintenance attributes (e.g., MTTR vs. mean cost of repair). Additionally, metrics are typically only useful within their collected domain, as across domains there are differences in how metrics are collected and the start and stop points for the timers associated with metrics, limiting their utility in examining the larger support and maintenance processes and costs across disparate, but related, systems.

The creation of an integrated maintenance system enables the standardization of metric definitions as well as the collection of maintenance-specific metrics to enable true lifecycle cost analyses as well as the execution of statistical analyses on the costs (monetary and operational) of specific components across multiple systems.

7.5.1 Standard Metric Definitions

Traditionally, maintenance systems deal in basic, well-defined metrics, such as A_0, A_i, A_t, MDT, MTBF, and MTTR. These and other metrics typically used as part of the maintenance lifecycle and which form the basis of reliability, maintainability, and availability engineering efforts during system design can be found in Appendix B, Key Operational Metrics. Of concern in any quantitative system are the units of measure and the definitions of the measurement. However, the operational and maintenance definitions of the metrics vary, according to systems. For instance, in some systems, the mean time to repair AFTER the fault is isolated, while in other systems, it is calculated once a fault has been confirmed. Therefore, at the surface, the system that measures MTTR after the fault is isolated will always have better metrics than the site that measures MTTR at failure. This would lead to the erroneous conclusion that the second site has better maintenance processes and procedures, when in fact, that is not a priori true. What is true is that they are measuring a smaller unit of time for a given failure. Similarly, in some systems down time EXCLUDES scheduled maintenance, while in other systems downtime INCLUDES scheduled maintenance. Therefore, a key benefit of the integrated maintenance system is the establishment of a common set of baseline metrics and common definitions of those metrics. Mean down time for any system supported by the integrated maintenance system is measured in the same way, enabling comparison of maintenance procedures and process improvements.

7.5.2 Maintenance-Oriented Metrics

While traditional reliability, maintainability, and availability metrics are critical to monitoring system status and health, they are not useful in calculating the cost effectiveness of a given maintenance approach, nor are they necessarily useful in root cause analysis. The lack of utility is not a fault in the metric per se, but in the fact that a metric only measures what it is supposed to measure and the vast majority of maintenance metrics are, in fact, truly operational metrics. Maintenance metrics should measure the effectiveness, cost, and value add of maintenance tasks, and while they should be tied to operational metrics like MTBF, they should be focused on the maintenance mission not the operational mission. For example, if the maintenance system has a quantitatively proven reliable process for repairing a particular defective part, yet operational sites experience high defect rates in the part, then we can investigate a few highly likely scenarios, such as:

- The operational environment is out of the range allowed
- The part is damaged in the logistics chain
- The part is improperly installed

Without the collection of maintenance specific metrics, there is no basis for starting at any point in the maintenance chain than the start of the repair cycle. Further, the operational site may start demanding new, rather than repaired parts, increasing costs. The investigation of the high MTBF for the part becomes politically charged as the operators and maintainers each blame the other because there is no metric beyond MTBF.

One example of a maintenance-oriented metric that can be collected as the result of the creation of an integrated maintenance system is “mean downtime per vendor product per unit time.” This metric calculates how often downtime is caused by a particular product[23] within a particular time window. This measurements enables the IMMOC to analyze the maintenance costs attributable to particular components and provide that analysis back to the acquisition community for consideration in future programs. Further, the analysis can be used to execute a cost/benefit analysis for switching providers of a particular component. Traditionally, the cost of switching vendors is viewed as prohibitive due to the operational impact, the cost of the new product, and the investment in the current product. However, the hypothetical “mean downtime per vendor product per unit time” metric enables the IMMOC to calculate the maintenance costs of using the current product and use that to offset potential costs associated with switching, if so desired.

Calculation of lifecycle maintenance costs is critical to the stated goal of reducing lifecycle costs associated with acquiring new systems. Within many USG development procurements there are clauses indicating that the cost analysis approach is based on “best value, to include lifecycle costs.” This language, while well intentioned, is meaningless if there is no data to backup the lifecycle costs. In the case of space-based systems, the operational life can extend decades, rapidly exceeding even the most expensive of development products. Therefore, while there is incentive to reduce development costs on the part of industry to be cost-competitive and win new business, the USG needs to focus more heavily on the lifecycle and maintenance costs of any development effort. The creation of the IMMOC and the integrated maintenance system enables the collection of data to support true lifecycle costs associated with maintenance.

7.6 Synergies

While the potential cost savings may provide sufficient reason for a feasibility analysis it is not sufficient to overcome the inertial resistance to the significant change represented by an integrated maintenance system. It will be the synergies created by the integrating the maintenance segments into a maintenance system that will provide additional benefits that not only help overcome the institutionalized resistance but will also provide justification for the initial costs associated with implementing the integrated maintenance concept.

[23] In this context product refers to any discrete component, to include modules and subassemblies as well as actual products sold as either COTS or GOTS.

7.6.1 Central Knowledge Base

A key component of the integrated maintenance system is its' centralized knowledge base. In addition to consolidation and centralized management of data, this repository provides enterprise level data mining capability.

Centralized management of the data ensures that all appropriate safeguards, access controls and record preservation requirements are consistently applied. This ensures that it is not possible to circumvent security restrictions enforced on data at various levels of aggregation. For example the system is able to prevent the disclosure funding levels for individual programs if the aggregate funding level is restricted. This would prevent identification of the restricted information (the aggregate funding level for all maintenance actions) from deduced through knowledge of the individual funding levels of various programs. Additionally centralized management ensures that individuals that do have a need to know information do not have to worry about making sure that they have not missed a data source. The centralized management ensures that all data is available to those that have a need to know it and that it is hidden from those without such a need.

A second benefit to the system is the data mining capability. The centralized data repository can be exploited in various ways.

7.6.1.1 Identification and prevention of future problems:

Due to the varied nature of the system supported by the integrated maintenance system it is reasonable to expect that these system will have been in operation for various lengths of time. The centralized knowledge base allows younger systems to gain the benefit of the root cause and trend analysis performed on the older systems. This information is then used to create a new maintenance plan that prevents/avoids these maintenance issues.

7.6.1.2 Trend Analysis

Due to the growing reliance on COTS and GOTS components there is a larger percentage of shared components in use among the system supported by the integrated maintenance system. Individual system may utilize only a small number of these components when looking across all systems there is a significant number. An individual system therefore may be unable to perform a trend analysis on maintenance actions due to the small sample size available, but the centralized knowledge base can look across all systems to perform the trend analysis.

7.6.1.3 Institutionalized Knowledge

In following with ITIL and CMMi best practices the knowledge base respresents an permanent source of information maintained independently of any individual. By consolidating the information associated with maintenance actions, baseline changes, and the internal workflows, the system ensures that information is preserved for staffing changes as well as for analysis and continual process improvement

7.6.2 Cost Savings

The integrated maintenance system has the potential to offer a number of proven cost saving measures that are typical results of consolidation efforts. These include savings from reduction in unused excess capacity throughout the system. Excess capacity will typically take the form of redundant facilities and staff and attendant infrastructure costs. A second source of savings is the increased efficiencies available to increased economies of scale. This will typically take the form of lower per capita costs associated with both management, facilities and logistics infrastructure.

In addition to the consolidation cost savings the integrated maintenance system is also in a position to offer savings to both ongoing maintenance costs as well as new system acquisition costs. This is because the integrated maintenance system will be able to negotiate enterprise maintenance agreements, which can influence new system development. Additionally because of the centralized knowledge base the integrated maintenance system can provide more accurate and complete maintenance lifecycle costs for particular components for systems that are in the development and planning phases. This lifecycle cost factors in not only fixed costs such as facilities or components but also variables costs such as logistics and labor.

These combined savings will allow the integrated maintenance system as a whole to provide more and better services than the aggregation of the individual maintenance segments could provide

7.6.3 Cross Training

As with any maintenance system the quality of the repairs and other maintenance actions are highly dependent on the skill set of the individuals performing the work. Through cross training the integrated maintenance system will be able to ensure that there is always a skilled resource supply necessary to provide maintenance on supported systems. As more and more systems leverage the user of COTS and GOTS components and sub assemblies it is possible to provide resource training that only needs to cover the transition from the default use of the part/subassembly to the specifics of the supported system, rather than the entire system. This common knowledge base can then be leveraged to allow an organic path within the maintenance facilities to transfer skills from senior members to more junior members. This common skill base also supports the ability of the integrated maintenance system to provide surge support as resources from similar systems can quickly be brought in and work with the more senior members of a specific maintenance shop to provide supplementary capabilities as needed.

In addition to establishing a skills baseline through the knowledgebase repository it is possible to integrate the cross training of individuals into their daily workflow either by assigning work case reviews and through work assignment routing to ensure that backup facilities are regularly included in maintenance tasks and do not lose their skill set or certifications.

7.6.4 Disaster Recovery and Continuity of Operations

It is the goal of any maintenance segment to ensure that the operational system being supported is available to fulfill its mission. With the increasingly global demand of operational systems this becomes a 24x7x365 need. In the traditional maintenance model where the maintenance segment is provisioned entirely as part of the operational system this can lead to either a shortage of funding or capability due to the significant cost associated with providing the ability to provide this level of maintenance services. It is in this kind of arena where the benefits of an integrated maintenance system are realized and one of the primary sources of future cost savings and service enhancements.

Through consolidation of the numerous independent maintenance segments the integrated maintenance system is able to plan for and provide disaster recovery and continuity of maintenance operations. Because the cost of facilities and logistics is now spread among numerous systems instead of a single system, the economies of scale allow for multiple facilities capable of supporting multiple systems. Through the integrated Command & Control structure these work actions can be automatically rerouted to different facilities. These facilities can utilize independent water, power, and communication grids as well as their own manpower resources. This becomes an organic capability of the distributed nature of the integrated maintenance system instead of the standard parallel but used only in the event of emergency paradigm. The integrated maintenance system is designed to include the surge capability as part of its function and can reutilize this to organically provide disaster recovery and continuity of operations.

8.0 Future Work

This study identifies numerous projects for future work. In addition to the specific items identified in Section 3.4, *Open Issues*, the conclusions identify numerous addition actions that should be performed as the immediate follow-on to this work:

1. Engage in a study of the costs of COTS and GOTS components for a satellite mission ground stations based on legacy systems and new systems that have introduced COTS and GOTS to replace custom developed software.
2. Begin construction of stochastic models for:
    a. Space-based system incident occurrence
    b. Personnel attrition in the maintenance chain
    c. Likelihood of problem or incident resolution at a particular level of the maintenance chain
3. Begin construction of models for:
    a. Communications infrastructure costs
    b. Computing resources based on the initial data model provided as part of this study
    c. Integer optimization for the number of maintenance sites
    d. Models for suitability of locations for maintenance sites
4. Expand the initial data model and architecture diagrams
5. Begin exploration of the feasibility of combining funding streams from multiple programs into a single maintenance funding stream or influencing the appropriations process to allocate integrated maintenance money during system acquisition appropriations.
6. Define MOEs for the integrated maintenance system

Appendix A Glossary Key System and Study Definitions

A.1 Communications Subsystem

This subsystem is responsible for control over all communication pipes (both logical and physical) used by the integrated maintenance system.

A.2 Control Subsystem

This subsystem is responsible for the Command & Control component of the integrated maintenance system. In addition to coordinating external commands from either operational systems or system owners the control subsystem is capable of positive control to ensure proper functioning of the integrated maintenance subsystem. This includes but is not limited to actions such as automatic rescheduling of work based on resource availability and initiating surge actions.

A.3 Depot

A depot represents any node maintenance chain that is not a terminal node (that is it is not a site or factory). There may be any number of depots in the chain. Each depot is capable of performing some level of maintenance to the system and knows what the next node in the chain is as well as what nodes it directly supports. Depots may be connected laterally to allow for resource sharing and routing.

A.4 External Design Support Subsystem

This subsystem is intended to support both the integrated maintenance system in its capacity planning and integration with COTS and GOTS products in addition to providing analysis capability to the New System Planner Interface.

A.5 External Auditor

This refers to any entity that has the authority to request/perform an audit of the integrated maintenance system or the records of any system maintained by the integrated maintenance system. These are listed as a primary relationship in support of requirement 4.5.2.

A.6 External Auditor Interface

This subsystem is responsible for interfacing with external auditors and law enforcement / investigative agencies. This is because from the perspective of the integrated maintenance system the only difference between a request from an external auditor and one from a law enforcement or investigative agency is in the scope and level of detail available to the requestor. Because all interfaces restrict access based on operational policy there is no need to provide a separate interface to support these two entities. This interface will not be responsible for the data generation or aggregation of the information requested, instead it will rely on the reporting subsystem, and appropriate shared resources to provide the necessary information. The interface will provide presence information for both the external users as well as the requested information. This interface provides both real time and non real time information and status as determined by operating policy.

A.7 External Vendors

This represents the COTS or GOTS vendors that are the ultimate end for any COTS and GOTS components that are part of the maintained systems. Due to the increasing use of COTS or GOTS products in operational systems this ensures that there the ability to include COTS or GOTS maintenance trails as needed, per requirement 4.4.2.

A.8 Factory

A factory represents the termination point of a maintenance chain of activities. It is the root node of the maintenance tree. While a system may be able to be serviced by many factories there is one and only one factory with primary responsibility for servicing that system all others are secondary and will only receive work packages for systems they are not the primary for if the primary factory routes the workload to the secondary. A factory may be the primary for multiple systems.

A.9 Factory Subsystem

This is the logical representation of factories in the integrated maintenance system.

A.10 Integrated Maintenance

Each maintenance chain is an independent tree. The thing that makes the system "integrated" is the IMMOC. It is the linkage between the trees whether that tree is linked at the factory (or root) level via secondary factory status or by the identification of shared capabilities of depots.

A.11 Knowledgebase Subsystem

This system is responsible for all permanent data storage in the integrated maintenance system and all access controls on that data.

A.12 Logistics Delay Time

Logistics delay time is the period of down time during which no maintenance takes place due to the time spent obtaining and delivering parts and services.

A.13 Logistics Subsystem

This subsystem is the logical representation of a logistics capability in the integrated maintenance system. It is responsible for maintaining and coordinating all transportation and storage needs of the integrated maintenance system.

A.14 Maintenance Chain

A maintenance chain is a complete hierarchy from the operational system (the site) to the primary factory. Each node on the maintenance chain has a clear delineation of responsibility and authorization to perform certain maintenance actions. For purposes of the chain only the primary path from site to factory needs to be considered. Any peer nodes are assumed to be acting on behalf of the primary node.

A.15 Maintenance Thread

A maintenance thread is a set of maintenance activities that is capable of being performed on a system. Each link in the maintenance chain is responsible for performing the activities appropriate to that level. A thread may either originate from a site and flow up the chain (in the case of a operator/preventive maintenance initiated thread) or from the factory down (in the case of an upgrade/replacement or commanded maintenance)

A.16 New System Planners

This refers to any entity that is using the integrated maintenance system to perform either capacity planning for a current system or developing a new system. It is the intent that the integrated maintenance system will assist in providing maintenance plans and estimates for the new system. This will allow the integrated maintenance system to perform capacity-planning activities as well as support the organizational requirements 4.1.1 and 4.1.2.

A.17 New System Planner Interface

This interface is to be used in conjunction with researcher interface to support planners/designers of new systems. This will allow planers access to appropriate maintenance information and provide the integrated maintenance system with future capacity requirements.

A.18 Operational Site Interface:

This subsystem is responsible for interfacing with operational systems maintained by the integrated maintenance subsystem. Unlike the system owner interface which is intended to interact with the human system owners this interface is to allow automation between (semi-) autonomous systems, the operational system, and the integrated maintenance system. This interface allows an operational system to request a maintenance action, request information about a maintenance action, be notified of certain events in the processing of a maintenance action, as well as inform the maintenance system of its status.

A.19 Operational System

This refers to any operational system that receives maintenance from the integrated maintenance system. The primary interaction with the integrated maintenance system will be through maintenance actions that requested from the integrated maintenance system and the over watch mission requirement 4.5.1.

A.20 Outsourced Maintenance Systems

This represents any maintenance activities that are not performed by the integrated maintenance system or the original vendor. It is intended to support future growth and as well as to differentiate COTS or GOTS maintenance trails from internal government maintenance trails (for example for crypto modules).

A.21 Overwatch Subsystem

This subsystem is responsible for all monitoring the status of both supported operational systems as well as the integrated maintenance system itself. This subsystem includes both passive (push) monitoring as well as active (pull) monitoring. Additionally this subsystem is responsible for alerting appropriate other interfaces/subsystems of events in accordance with operational policy. For example while the control over and use of storage facilities is part of the logistics subsystem; the Overwatch subsystem is responsible for notifying other subsystems when the storage facility reaches a threshold of capacity.

A.22 Physical Location

For our purposes physical location is irrelevant to the status of sites, depots, or factories. Even if the depot is collocated within the same physical building as the operational system, it is still considered two distinct logical entities the "site" which consists of the system and the operators and a "depot" which consists of the maintenance staff. This is because as leaf nodes the IMMOC does not have visibility into the site beyond standard reporting (it has no control and is subject to the constraints of the site when attempting to perform ordered maintenance activities) while it does have visibility into the depot.

A.23 Repair Depots Subsystem

This is the logical representation of depots in the integrated maintenance system. As the integrated maintenance system is responsible for maintain itself this subsystem is also operational support of the integrated maintenance system itself.

A.24 Reporting Subsystem

This subsystem is responsible for the aggregation and dissemination of all structured data throughout the integrated maintenance system.

A.25 Researcher

The represents any entity that is performing research/analysis on either maintenance processes or the policies of the integrated maintenance system itself allowing cross system analysis that is not possible in a stovepipe maintenance process. This is in keeping with best practices that will allow integrated maintenance system to optimize its services as identified in requirements 4.5.1.3 and 4.5.1.2.

A.26 Researcher Interface:

This interface supports researches in performing analysis on operational systems supported by the integrated maintenance system and the integrated maintenance system itself. This is interface will provide data and access restricted by operational policy by interacting with the knowledgebase, reporting, tracking and simulation subsystems.

A.27 Shared Resources Subsystem

This subsystem is responsible for coordinating access to shared resources. This includes both equipment and personnel that are capable of supporting/existing at multiple physical locations or being used by multiple subsystems. For example while the communications subsystem is responsible for actually transmitting data on a communications link it is the shared resources subsystem that is responsible for ensuring that all subsystems have appropriate access to the communications link itself.

A.28 Site

A site is the leaf node of a maintenance tree and the origin of the maintenance chain. Maintenance starts at the site and escalates to the factory at the root of the maintenance chain. For our purposes the site is composed of system operators and not maintenance staff. While there are numerous maintenance activities that may be performed at the site they are outside of the visibility of the IMMOC. That is not to say that the IMMOC is not aware of the activities or status of the system at the site but that it is not involved in the operator initiated/performed maintenance unless that activity results in an escalation to a depot (at which point the previous activities are part of the history). This means that equipment and such that is owned by the "site" is not part of the IMMOC inventory or logistics. For example, if a "site" keeps five spare parts on hand, which the operator is able to swap out when a certain Light Emitting Diode (LED) turns red, then the spare parts are not visible to the IMMOC once at the site, unless they are returned for maintenance. The fact that the parts were ordered from the depot and the record of the order and shipment will be visible to the IMMOC. However if the site has to request the spare from "maintenance" (the depot in our terms) then it would be a maintenance activity that is recorded and within the IMMOC purview.

A.29 System Owners

This refers to any entity that has control over either the integrated maintenance system itself or any system maintained by the integrated maintenance system. System owners along with the Operational Site represent the primary interactions for the over watch mission requirement 4.5.1.

A.30 System Owner Interface:

This subsystem is responsible for interfacing with system owners. These include the owners of operational systems supported by the integrated maintenance system as well as the owners of the integrated maintenance system itself. In support of this the interface primarily interacts with the reporting subsystem to provide appropriate information to the system owners as well as to the control system to process any commands from system owners. This subsystem is an active interface capable of initiating interaction (via sending information without an explicit request) as required by operational policy.

A.31 Vendor and Outsourced Maintenance Interfaces

This interface supports the Vendor and Outsourced Maintenance external systems. These interfaces are for access from the integrated maintenance system into the appropriate external maintenance system. This allows the integrated maintenance system to maintain information and visibility (as determined by service level agreements) along the entire maintenance trail. Secondly, this interface provides the ability for the integrated maintenance system to execute “data calls” as determined by operational policy. These data calls may be triggered by an external request or by the integrated maintenance as part of its normal operations (for example in response to a low inventory threshold).

A.32 Workflow Tracking Subsystem

This subsystem is responsible for tracking a maintenance action throughout integrated maintenance system. This subsystem is similar to the Overwatch subsystem but focused on tracking an actions progress/status within the integrated maintenance system.

Appendix B Key Operational Metrics

B.1 Achieved Availability (A_a)

Achieved availability (A_a) is similar to inherent availability except that corrective maintenance and preventive maintenance of the system is now included. Equation 2 shows the calculation of achieved availability based on Meant Time Between Maintenance (MTBM) and Mean Time to Repair (MTTR)

$$A_a = \frac{MTBM}{MTBM + MTTR}$$

Equation 2: Calculation of Achieved Availability

B.2 Administrative Delay Time

Administrative delay time is the period of down time during which no maintenance takes place due to delays in administrative processing, assignment of maintenance personnel or equipment and transportation.

B.3 Down Time

Down time is the accumulated time that the equipment is not mission effective due to failure. This includes all time required for scheduled maintenance and off-board logistics delay and repair of operational mission failures.

B.4 Inherent Availability (A_i)

Inherent availability (A_i) is directly related to the design of the equipment and is calculated from the system Mean Time Between Failures (MTBF) and MTTR. Equation 3 shows the calculation of Inherent Reliability. Inherent availability excludes preventive maintenance, scheduled maintenance and logistics delay times.

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Equation 3: Calculation of Inherent Availability

B.5 Instantaneous (Point) Availability (A_t)

Instantaneous or Point availability (A_t) is the probability that a system (or component) will be operational (up and running) at any random time, t. This is very similar to the reliability function in that it gives a probability that a system will function at the given time, t. However, unlike reliability, it incorporates maintainability and logistics information, as it includes repairs completed prior to the time of interest. An example of instantaneous availability is the probability of a piece of maintenance equipment being able to complete a maintenance action at a specific time during the execution of a maintenance thread.

B.6 Mean Availability ($\overline{A(t)}$)

Mean availability or average uptime is the proportion of time during a mission or other period of time that the given system is available for use. It represents the mean value of the instantaneous availability between (0,t]. Equation 4 shows the calculation of mean availability as the integral of A_t over the interval (0,t].

$$\overline{A(t)} = \frac{1}{t}\int_0^t A(u)du$$

Equation 4: Calculation of Mean Availability

B.7 Mean Down Time (MDT)

The Mean Down Time (MDT) is the summation of all down times including logistics and administrative delay time

B.8 Mean Time Between Critical Failure (MTBCF)

MTBCF is the period between which the system is non-operational due to a failure and the next critical failure that renders the system non-operational. MTCBF is a measure of mission reliability. Equation 5 shows the calculation for MTBCF based on the reliability of the system as a whole, which is highly dependent on the availability of spares. R_{sys} must be analytically determined based on the reliability engineering and analysis of the given system.

$$MTBCF = \frac{\int_0^T R_{sys}(t)\,dt}{1 - R_{sys}(T)}$$

Equation 5: Calculation of MTBCF

B.9 Mean Time Between Failures (MTBF)

MTBF is the period between any service or system restoration and the next failure of that service or system. MTBF is a measure of serial or logistic reliability. Equation 6 shows the calculation for MTBF in where λ is the failure rate for a given piece of equipment.

$$MTBF = \frac{1}{\sum_{i=1}^{N} \lambda_i}$$

Equation 6: Calculation of MTBF

B.10 Mean Time Between Maintenance (MTBM)

Mean Time Between Maintenance is the period of time between scheduled maintenance actions.

B.11 Mean Time Between Service Incidents (MTBSI)

The period of time between the detection of a given incident for a system or service and the detection of the next incident (of the same or different type) for the same system or service.

B.12 Mean Time To Failure (MTTF)

MTTF is a special case of MTBF reflecting the expected time to the failure of an item or system. MTTF is often applied to non-repairable equipment and systems and reflects the occurrence of a failure event as defined for the item and is the reciprocal of the item’s failure rate.

B.13 Mean Time To Repair (MTTR)

The time between the detection of a failure or incident in a service or system and the restoration of that system or service to operational status.

B.14 Mean Time To Restore Functionality (MTTRF)

MTTRF is the average time taken to restore functionality across all critical system failures (failures that impact system operations).

$$MTTRF = \frac{\sum Critical\,\mathrm{Re}\,storeTime}{Number\,of\;Critical\;Failures}$$

Equation 7: Calculation of Mean Time to Restore Functionality

B.15 Mission Capable Rate (MCR)

Mission Capable Rate is the percent of time that the system is able to perform ANY of its missions. Survivability missions are excluded since they provide no unique mission functionality, but merely maintain the system in a minimal state to prevent total mission loss. Survivability states enable further repairs or transition to a more operational state when external conditions enable.

$$MCR = \frac{System\,Life\,Time - \ Down\ Time}{System\,Life\,Time} * 100$$

Equation 8: Calculation of Mission Capability Rate

B.16 Operational Availability (A_0)

Operational availability (A_0) is a user-oriented assessment of the system's availability and accounts for other all sources of "downtime." Operational availability is very dependent on the logistics approach and limitations on what is chargeable as Logistics Delay Time. A_0 data are snapshots per unit time, not cumulative trending.

$$A_O = \frac{UpTime}{UpTime + DownTime}$$

Alternately,

$$A_o = \frac{MTBM}{MTBM + MDT}$$

Equation 9: Calculation of Operational Availability

B.17 Operational Dependability (D_0)

Operational Dependability (D_0) is a user oriented assessment of the system's dependability and represents the percentage of time that the system is available for normal operations.

$$D_0 = \frac{MTBCF}{MTBCF + MTTRF}$$

Equation 10: Calculation of Operational Dependability

B.18 Steady State Availability ($A(\infty)$)

Steady state availability ($A(\infty)$) is the limit of average availability as time approaches infinity, as illustrated by Equation 11.

$$A(\infty) = \lim_{t \to \infty} A(t)$$

Equation 11: Calculation of Steady State Availability

B.19 Up Time

Up time is the accumulated time that the equipment meets its performance requirements, or the total time that the system or equipment is considered operating to its requirements. Uptime is defined as the same as operating time.

Appendix C Industry Best Practices in Metric Selection and Collection

In conjunction with Figure 6.4-1, Table C-1 highlights some of the key considerations that Gartner and Burton Group make with regard to the identification and collection of metrics in operations and maintenance environments. Specific considerations include understanding the difference between public metrics, shared with organizations external to the maintenance organization and internal metrics used for planning purposes as well as the requirement to focus on process outcomes, not process execution.

Table C-1: Key Considerations in Metric Collection for Maintenance Systems

No.	Key Consideration	Source	Title	Date
1	"A critical mistake made by IT organizations attempting to measure and communicate performance is the failure to differentiate the measures to share with business customers and the measures that should be used only internally. Getting this distinction right is an essential underpinning to IT organizational credibility."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
2	"Before an IT organization can identify an appropriate set of metrics, it must articulate a service portfolio."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
3	"Although every IT organization may offer essentially the same services, the way those services are bundled, positioned, perceived, and executed is unique to every business. Thus, standardized service and process metrics essentially don't exist, and IT organizations must design their own."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
4	"The only reason to measure anything is to ensure that desirable outcomes are achieved. All IT metrics, therefore, should be aligned to the services IT organizations offer and the business contribution those services make."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
5	SLAs should focus on service outcomes, not process-oriented metrics	Gartner	A Framework for Designing IT Service and Process Metrics	2006
6	Develop a Service-to-Process Map	Gartner	A Framework for Designing IT Service and Process Metrics	2006
7	"Every process involved in service delivery must have its outcomes measured."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
8	"It may…be desirable to implement real-time measurement and monitoring against key processes to enable proactive process improvement before service levels dip…"	Gartner	A Framework for Designing IT Service and Process Metrics	2006
9	"Metrics that are appropriate for customers are focused on business benefits."	Gartner	A Framework for Designing IT Service and Process Metrics	2006

10	"Metrics that are appropriate for monitoring and diagnosis are for IT organizations."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
11	"Metrics and measurement systems are not static. As services, processes and capabilities change, so must SLAs and process outcome metrics."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
12	"Measure only when necessary. Measurement for the sake of measurement or measurement that is unfocused represents a cost to the business with no commensurate benefit."	Gartner	A Framework for Designing IT Service and Process Metrics	2006
13	Measure what you care about - Quantify “quality” - People will spend time and money optimizing whatever you measure; don't measure the wrong thing	Burton Group	Burton Group Presentation, "Establishing an Enterprise-wide Measurement Infrastructure,"	16 May 2006
14	Measure at demarcation points - Assign responsibility to organizations - Assist in rapid incident diagnosis ("triage")	Burton Group	Burton Group Presentation, "Establishing an Enterprise-wide Measurement Infrastructure,"	16 May 2006
15	Use appropriate validation tools and statistical treatment - For "key performance indicator" metrics, validate measurement accuracy and use the appropriate statistics	Burton Group	Burton Group Presentation, "Establishing an Enterprise-wide Measurement Infrastructure,"	16 May 2006
16	Ensure there is a relationship to controllable behavior - How will you fix a problem indicated by the metrics? - What data is needed for diagnosis?	Burton Group	Burton Group Presentation, "Establishing an Enterprise-wide Measurement Infrastructure,"	16 May 2006
17	"SLA metrics should be chosen based on simplicity - high service levels on items of importance - rather than on an exhaustive list of interesting measurements. Critical success factors for SLAs center on the balanced-scorecard approach, including fewer impact-driven metrics, consistent tracking and reporting, and a selection of metrics that are meaningful to end-user constituencies."	Meta Group	"Service Level Agreements," Meta Group	2002

Appendix D Metrics Mapped to Operational Balanced Score Card Quadrants

Table D-1: Key Metrics and Their Balanced Scorecard Quandrant

No	Performance Measures	Source	Balanced Scorecard Quadrants			
			Financial Evaluation / Organizational Contribution	Customer Satisfaction / User Orientation	Internal Processes / Operational Excellence	Ability to Innovate / Future Orientation
1	Workload analysis	ITIL/Service Support/Service Desk: Incident Reporting & Review			X	
2	Areas requiring escalation by group	ITIL/Service Support/Service Desk: Incident Reporting & Review			X	
3	Possible service breaches	ITIL/Service Support/Service Desk: Incident Reporting & Review			X	
4	All outstanding incidents	ITIL/Service Support/Service Desk: Incident Reporting & Review			X	
5	Service Availability	ITIL/Service Support/Service Desk: Incident Reporting & Review			X	
6	Major Incident areas that occur the most often, staff spend the most time working on, take the longest time to turn around to the customer	ITIL/Service Support/Service Desk: Incident Reporting & Review			X	
7	Related Incidents	ITIL/Service Support/Service Desk: Incident Reporting & Review			X	

8	Known Errors and required changes	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
9	Service Breaches	ITIL/Service Support/Service Desk: Incident Reporting & Review		**X**	**X**	
10	Customer Satisfaction	ITIL/Service Support/Service Desk: Incident Reporting & Review		**X**		
11	Trends, major services affecting the business	ITIL/Service Support/Service Desk: Incident Reporting & Review	**X**			
12	Staff workloads	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
13	Areas requiring escalation by group	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
14	Possible service breaches	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
15	All outstanding incidents	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
16	Overall performance, achievements and trend analyses	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
17	Individual service target achievements	ITIL/Service Support/Service Desk: Incident Reporting & Review		**X**		
18	Customer perceptions and levels of satisfaction	ITIL/Service Support/Service Desk: Incident Reporting & Review		**X**		

19	Customer training and education needs	ITIL/Service Support/Service Desk: Incident Reporting & Review				**X**
20	Support staff and third-party performance	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
21	Application and technology performance	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
22	Content of review and reporting matrix	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
23	Cost of service provision/failure	ITIL/Service Support/Service Desk: Incident Reporting & Review	**X**			
24	Planned changes for the following week	ITIL/Service Support/Service Desk: Incident Reporting & Review				**X**
25	Major incidents/problems/changes from the previous week, along with any work-arounds, fixes, etc.	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
26	"Unsatisfied" customer incidents from previous weeks	ITIL/Service Support/Service Desk: Incident Reporting & Review		**X**		
27	Previous weeks' poorly performing infrastructure items (e.g. server, network, application)	ITIL/Service Support/Service Desk: Incident Reporting & Review			**X**	
28	Total number of incidents	ITIL/Service Support/Incident Management			**X**	
29	Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code	ITIL/Service Support/Incident Management			**X**	
30	Percentage of incidents handled within agreed response time (incident response-time targets may be	ITIL/Service Support/Incident Management		**X**		

	specified in SLAs, for example, by impact code)					
31	Average cost per incident	ITIL/Service Support/Incident Management	**X**			
32	Percentage of incidents closed by the Service Desk without reference to other levels of support	ITIL/Service Support/Incident Management			**X**	
33	Incidents processed per Service Desk workstation	ITIL/Service Support/Incident Management			**X**	
34	Number and percentage of incidents resolved remotely, without the need for a visit	ITIL/Service Support/Incident Management			**X**	
35	The number of RFCs raised and the impact of those RFCs on the availability and reliability of the services covered	ITIL/Service Support/Problem Management			**X**	
36	The amount of time worked on investigations and diagnoses per organizational unit or supplier, split by Problem types	ITIL/Service Support/Problem Management			**X**	
37	The number and impact of incidents occurring before the root Problem is closed or a Known Error is confirmed	ITIL/Service Support/Problem Management			**X**	
38	The ratio of immediate (reactive) support effort to planned support effort in Problem Management	ITIL/Service Support/Problem Management			**X**	
39	The plans for resolution of open Problems with regard to resources: people, other used resources, costs (against budget)	ITIL/Service Support/Problem Management			**X**	
40	Short description of actions to be undertaken	ITIL/Service Support/Problem Management			**X**	
41	The number of Problems and errors split by status, service, impact, category, user group	ITIL/Service Support/Problem Management			**X**	
42	Total elapsed time on closed Problems	ITIL/Service Support/Problem Management			**X**	

43	The elapsed time to date on outstanding Problems	ITIL/Service Support/Problem Management			**X**	
44	The mean and maximum elapsed time to close Problems or confirm a Known Error, from the time of raising the Problem record, by impact code and by support group (including vendors)	ITIL/Service Support/Problem Management			**X**	
45	Any temporary resolution actions	ITIL/Service Support/Problem Management			**X**	
46	The expected resolution time for outstanding Problems	ITIL/Service Support/Problem Management			**X**	
47	The total elapsed time for closed Problems	ITIL/Service Support/Problem Management			**X**	
48	Accurate information of configuration items (CIs)	ITIL/Service Support/Configuration Management			**X**	
49	The number of Changes implemented in the period, in total and by CI, configuration type, service, etc.	ITIL/Service Support/Change Management			**X**	
50	A breakdown of the reasons for Change (user requests, enhancements, business requirements, service call/Incident/Problem fixes, procedures/training improvement, etc.)	ITIL/Service Support/Change Management			**X**	
51	The number of Changes successful	ITIL/Service Support/Change Management			**X**	
52	The number of Changes backed-out, together with the reasons (e.g. incorrect assessment, bad build)	ITIL/Service Support/Change Management			**X**	
53	The number of Incidents traced to Changes (broken down into Problem-severity levels) and the reasons (e.g. incorrect assessment, bad build)	ITIL/Service Support/Change Management			**X**	
54	The number of RFCs (and any trends in origination)	ITIL/Service Support/Change Management			**X**	

55	The number of implemented Changes reviewed, and the size of review backlogs (broken down over time)	ITIL/Service Support/Change Management			**X**	
56	High incidences of RFCs/PRs relating to one CI (these are worthy of special attention), giving the reasons (e.g. volatile User requirements, fragile component, bad build)	ITIL/Service Support/Change Management			**X**	
57	Figures from previous periods (last period, last year) for comparison	ITIL/Service Support/Change Management			**X**	
58	The number of RFCs rejected	ITIL/Service Support/Change Management			**X**	
59	The proportion of implemented Changes that are not successful (in total and broken down by CI)	ITIL/Service Support/Change Management			**X**	
60	Change backlogs, broken down by CI and by stage in the Change Management process	ITIL/Service Support/Change Management			**X**	
61	What number, or percentage, of services are covered by Service Level Agreements (SLAs)?	ITIL/Service Delivery/Service Level Management	**X**			
62	Are underpinning contracts and OLAs in place for all SLAs and for what percentage?	ITIL/Service Delivery/Service Level Management	**X**			
63	Are SLAs being monitored and are regular reports being produced?	ITIL/Service Delivery/Service Level Management	**X**			
64	Are review meetings being held on time and correctly minuted?	ITIL/Service Delivery/Service Level Management	**X**			
65	Is there documentary evidence that issues raised at reviews are being followed up and resolved (e.g. via a Service Improvement Program)	ITIL/Service Delivery/Service Level Management	**X**			
66	Are SLAs, OLAs and underpinning contracts current and what percentage are in need of review and update?	ITIL/Service Delivery/Service Level Management	**X**			
67	What number or percentage of service targets are being met and what is the number and severity of service breaches?	ITIL/Service Delivery/Service Level Management	**X**			

68	Are service breaches being followed up effectively?	ITIL/Service Delivery/Service Level Management	**X**			
69	Are service level achievements improving?	ITIL/Service Delivery/Service Level Management	**X**			
70	Are customer perception statistics improving?	ITIL/Service Delivery/Service Level Management		**X**		
71	Are IT costs decreasing for services with stable (acceptable but not improving) service level achievements?	ITIL/Service Delivery/Service Level Management	**X**			
72	Actual IT costs against budgeted IT costs	ITIL/Service Delivery/Financial Management	**X**			
73	Cost targets for performance and Service Delivery	ITIL/Service Delivery/Financial Management	**X**			
74	Return on Investment (ROI)	ITIL/Service Delivery/Financial Management	**X**			
75	Return on Capital Employed (ROCE)	ITIL/Service Delivery/Financial Management	**X**			
76	Total Cost of Ownership (TCO)	ITIL/Service Delivery/Financial Management	**X**			
77	Hardware costs	ITIL/Service Delivery/Financial Management	**X**			
78	Software costs	ITIL/Service Delivery/Financial Management	**X**			
79	People costs	ITIL/Service Delivery/Financial Management	**X**			
80	Accommodation costs	ITIL/Service Delivery/Financial Management	**X**			
81	External service costs	ITIL/Service Delivery/Financial Management	**X**			
82	Transfer costs	ITIL/Service Delivery/Financial Management	**X**			

83	Direct costs	ITIL/Service Delivery/Financial Management	**X**			
84	Indirect costs	ITIL/Service Delivery/Financial Management	**X**			
85	Trends of the current resource utilization	ITIL/Service Delivery/Capacity Management			**X**	
86	Estimate of the future resource requirement	ITIL/Service Delivery/Capacity Management				**X**
87	Models of the predicted changes in IT service	ITIL/Service Delivery/Capacity Management				**X**
88	Demand for IT services	ITIL/Service Delivery/Capacity Management		**X**		
89	Supply of IT services	ITIL/Service Delivery/Capacity Management			**X**	
90	SLM exceptions	ITIL/Service Delivery/Capacity Management			**X**	
91	Resource utilization exceptions	ITIL/Service Delivery/Capacity Management			**X**	
92	CPU utilization	ITIL/Service Delivery/Capacity Management			**X**	
93	Memory utilization	ITIL/Service Delivery/Capacity Management			**X**	
94	% CPU per transaction type	ITIL/Service Delivery/Capacity Management			**X**	
95	IO rates (physical and buffer) and device utilization	ITIL/Service Delivery/Capacity Management			**X**	
96	Queue length (maximum and average)	ITIL/Service Delivery/Capacity Management			**X**	
97	File store utilization	ITIL/Service Delivery/Capacity Management			**X**	

98	Transactions	ITIL/Service Delivery/Capacity Management			**X**	
99	Transactions per second (maximum and average)	ITIL/Service Delivery/Capacity Management			**X**	
100	Transaction response time	ITIL/Service Delivery/Capacity Management			**X**	
101	Batch duration profiles	ITIL/Service Delivery/Capacity Management			**X**	
102	Number of hits	ITIL/Service Delivery/Capacity Management			**X**	
103	Number of log-ons and concurrent Users	ITIL/Service Delivery/Capacity Management			**X**	
104	Number of network nodes in use (e.g. network devices, PCs, servers, etc.)	ITIL/Service Delivery/Capacity Management			**X**	
105	Capacity (throughput)	ITIL/Service Delivery/Capacity Management			**X**	
106	Performance (response times)	ITIL/Service Delivery/Capacity Management			**X**	
107	Total resource utilization level	ITIL/Service Delivery/Capacity Management			**X**	
108	Load that each service places on each particular resource	ITIL/Service Delivery/Capacity Management			**X**	
109	Baselines of the normal operating levels	ITIL/Service Delivery/Capacity Management			**X**	
110	Baselines for individual components	ITIL/Service Delivery/Capacity Management			**X**	
111	Baselines for specific services	ITIL/Service Delivery/Capacity Management			**X**	
112	User response times	ITIL/Service Delivery/Capacity Management			**X**	

113	Transaction rates	ITIL/Service Delivery/Capacity Management			**X**	
114	Distribution of workload across available resource	ITIL/Service Delivery/Capacity Management			**X**	
115	Utilization data for each component	ITIL/Service Delivery/Capacity Management			**X**	
116	Utilization data for each service	ITIL/Service Delivery/Capacity Management			**X**	
117	Mainframe: CPU utilization	ITIL/Service Delivery/Capacity Management			**X**	
118	Mainframe: Paging rates	ITIL/Service Delivery/Capacity Management			**X**	
119	Mainframe: I/Os per second	ITIL/Service Delivery/Capacity Management			**X**	
120	Application: No of transactions	ITIL/Service Delivery/Capacity Management			**X**	
121	Application: Response times	ITIL/Service Delivery/Capacity Management			**X**	
122	UNIX server: CPU utilization	ITIL/Service Delivery/Capacity Management			**X**	
123	UNIX server: memory utilization	ITIL/Service Delivery/Capacity Management			**X**	
124	UNIX server: No of processes	ITIL/Service Delivery/Capacity Management			**X**	
125	Middleware: Average queue lengths	ITIL/Service Delivery/Capacity Management			**X**	
126	Middleware: No of transactions serviced	ITIL/Service Delivery/Capacity Management			**X**	
127	Network: Bandwidth utilization	ITIL/Service Delivery/Capacity Management			**X**	

128	Network: No of connections	ITIL/Service Delivery/Capacity Management			**X**	
129	Network: Error rates	ITIL/Service Delivery/Capacity Management			**X**	
130	Database: Shared memory utilization	ITIL/Service Delivery/Capacity Management			**X**	
131	Database: No of queries per second	ITIL/Service Delivery/Capacity Management			**X**	
132	PC Client: CPU utilization	ITIL/Service Delivery/Capacity Management			**X**	
133	PC Client: Memory utilization	ITIL/Service Delivery/Capacity Management			**X**	
134	Changes to workloads	ITIL/Service Delivery/Capacity Management			**X**	
135	Growth in workload	ITIL/Service Delivery/Capacity Management			**X**	
136	Predictions/models of IT service behavior (analytical and simulations)	ITIL/Service Delivery/Capacity Management				**X**
137	Estimates of resource requirements	ITIL/Service Delivery/Capacity Management				**X**
138	Forecasts of resource requirements	ITIL/Service Delivery/Capacity Management				**X**
139	Forecasts of trends in resource utilization	ITIL/Service Delivery/Capacity Management				**X**
140	Performance and throughput of all services and components	ITIL/Service Delivery/Capacity Management			**X**	
141	Increase or decrease in panic buying	ITIL/Service Delivery/Capacity Management			**X**	
142	Forecasts of planned expenditure	ITIL/Service Delivery/Capacity Management				**X**

143	Ratio of IT capacity to business need	ITIL/Service Delivery/Capacity Management			**X**	
144	Lost productivity due to poor performance	ITIL/Service Delivery/Capacity Management			**X**	
145	Lost business due to inadequate Capacity	ITIL/Service Delivery/Capacity Management			**X**	
146	SLA targets	ITIL/Service Delivery/Capacity Management				**X**
147	Results of Component Failure Impact Analysis (CFIA)	ITIL/Service Delivery/Capacity Management				**X**
148	Results of Fault Tree Analysis (FTA)	ITIL/Service Delivery/Capacity Management				**X**
149	Ratio of people per desktop	ITIL/Service Delivery/Capacity Management			**X**	
150	Short, medium and long-term trends in resource usage, broken down by hardware platform	ITIL/Service Delivery/Capacity Management			**X**	
151	Forecasts of resource usage resulting from service forecasts	ITIL/Service Delivery/Capacity Management				**X**
152	Traditional IT Availability Measure: % Available	ITIL/Service Delivery/Availability Management			**X**	
153	Traditional IT Availability Measure: % Unavailable	ITIL/Service Delivery/Availability Management			**X**	
154	Traditional IT Availability Measure: Duration	ITIL/Service Delivery/Availability Management			**X**	
155	Traditional IT Availability Measure: Frequency of failure	ITIL/Service Delivery/Availability Management			**X**	
156	Traditional IT Availability Measure: Impact of failure	ITIL/Service Delivery/Availability Management			**X**	
157	Traditional IT Availability Measure: % Available	ITIL/Service Delivery/Availability Management			**X**	

158	User Availability: Frequency of downtime	ITIL/Service Delivery/Availability Management		**X**		
159	User Availability: Duration of downtime	ITIL/Service Delivery/Availability Management		**X**		
160	User Availability: Scope of impact	ITIL/Service Delivery/Availability Management		**X**		
161	User Availability: Impact by User minutes lost	ITIL/Service Delivery/Availability Management		**X**		
162	User Availability: Impact by business transaction	ITIL/Service Delivery/Availability Management		**X**		
163	Business driven measurements based on vital business functions (VBF)	ITIL/Service Delivery/Availability Management	**X**			
164	Availability: measures that demonstrate consequences of IT availability on vital business functions (VBF)	ITIL/Service Delivery/Availability Management	**X**			
165	Availability: measures of application services required to run the business operation and service User input	ITIL/Service Delivery/Availability Management			**X**	
166	Availability: measurement of data availability	ITIL/Service Delivery/Availability Management			**X**	
167	Availability: measures that reflect availability, reliability and maintainability of IT infrastructure components supplied and maintained by the IT support organization	ITIL/Service Delivery/Availability Management			**X**	
168	Availability: measures of the IT platform that ultimately supports the processing of the business application(s)	ITIL/Service Delivery/Availability Management			**X**	
169	Availability reports should include four dimensions: availability, reliability, maintainability and response times of an IT service or component	ITIL/Service Delivery/Availability Management			**X**	
170	Data pertaining to IT component downtime (planned and unplanned)	ITIL/Service Delivery/Availability Management			**X**	

171	Forecasts of availability	ITIL/Service Delivery/Availability Management				**X**
172	Results of CRAMM (risk analysis methodology)	ITIL/Service Delivery/Availability Management				**X**
173	Results of Systems Outage Analysis (SOA)	ITIL/Service Delivery/Availability Management			**X**	
174	Basic availability calculation ((AST - DT)/AST)X100	ITIL/Service Delivery/Availability Management			**X**	
175	Total infrastructure availability (serial configuration & parallel configuration)	ITIL/Service Delivery/Availability Management			**X**	
176	Calculations of the cost of unavailability	ITIL/Service Delivery/Availability Management	**X**			
177	Downtime (planned, actual, extended)	ITIL/Service Delivery/Availability Management			**X**	
178	Incident reporting: Mean Time Between Failures (MTBF)	ITIL/Service Delivery/Availability Management			**X**	
179	Incident reporting: Mean Time Between System Incidents (MTBSI)	ITIL/Service Delivery/Availability Management			**X**	
180	Incident reporting: Mean Time to Repair (MTTR)	ITIL/Service Delivery/Availability Management			**X**	
181	System Outage Analysis (SOA): Number of recommendations	ITIL/Service Delivery/Availability Management			**X**	
182	System Outage Analysis (SOA): Number of recommendations rejected	ITIL/Service Delivery/Availability Management			**X**	
183	System Outage Analysis (SOA): Number of recommendations completed	ITIL/Service Delivery/Availability Management			**X**	
184	System Outage Analysis (SOA): Number of recommendations in progress	ITIL/Service Delivery/Availability Management			**X**	
185	System Outage Analysis (SOA): Number of recommendations with no progress	ITIL/Service Delivery/Availability Management			**X**	

186	Measures of incident start	ITIL/Service Delivery/Availability Management			**X**	
187	Measures of incident detection	ITIL/Service Delivery/Availability Management			**X**	
188	Measures of incident diagnosis	ITIL/Service Delivery/Availability Management			**X**	
189	Measures of incident repair	ITIL/Service Delivery/Availability Management			**X**	
190	Measures of incident recovery	ITIL/Service Delivery/Availability Management			**X**	
191	Measures of incident restoration	ITIL/Service Delivery/Availability Management			**X**	
192	Results of a Technical Observation Post (TOP)	ITIL/Service Delivery/Availability Management			**X**	
193	Apdex (gaining popularity as a coarse “single number” Divides users into “satisfied,” “tolerating,” and “frustrated,” then weights them in the computation)	Burton Group Presentation, "Establishing an Enterprise-wide Measurement Infrastructure," May 16, 2006		**X**		
194	System Uptime	"Service Level Agreements," Meta Group, 2002			**X**	
195	Network Availability	"Service Level Agreements," Meta Group, 2002			**X**	
196	Programming Hours	"Service Level Agreements," Meta Group, 2002			**X**	
197	Help Desk Responsiveness	"Service Level Agreements," Meta Group, 2002		**X**		
198	Complaint Resolution	"Service Level Agreements," Meta Group, 2002		**X**		
199	Project Schedules	"Service Level Agreements," Meta Group, 2002		**X**		

200	Customer Satisfaction Metrics	"Service Level Agreements," Meta Group, 2002		**X**		
201	Server Availability	"Service Level Agreements," Meta Group, 2002			**X**	
202	Wide-Area Network (WAN) Availability	"Service Level Agreements," Meta Group, 2002			**X**	
203	Application Response Times	"Service Level Agreements," Meta Group, 2002			**X**	
204	Mainframe Response Times	"Service Level Agreements," Meta Group, 2002			**X**	
205	Network Latency	"Service Level Agreements," Meta Group, 2002			**X**	
206	Time to resumption of business after failure	"Service Level Agreements," Meta Group, 2002			**X**	
207	Time taken to complete an application modification request	"Service Level Agreements," Meta Group, 2002		**X**		
208	Meeting project schedules	"Service Level Agreements," Meta Group, 2002		**X**		
209	Metrics (number, percent, etc.) on up-to-date applications	"Service Level Agreements," Meta Group, 2002		**X**		
210	Number of reopened tickets	"Service Level Agreements," Meta Group, 2002		**X**		
211	Customer satisfaction regarding quality	"Service Level Agreements," Meta Group, 2002		**X**		
212	Customer satisfaction regarding performance	"Service Level Agreements," Meta Group, 2002		**X**		
213	Customer satisfaction regarding friendliness	"Service Level Agreements," Meta Group, 2002		**X**		
214	Customer satisfaction regarding professionalism	"Service Level Agreements," Meta Group, 2002		**X**		

215	Customer satisfaction regarding flexibility	"Service Level Agreements," Meta Group, 2002		**X**		
216	Customer satisfaction regarding competence	"Service Level Agreements," Meta Group, 2002		**X**		
217	Customer satisfaction regarding timeliness	"Service Level Agreements," Meta Group, 2002		**X**		
218	Network Uptime	"Service Level Agreements," Meta Group, 2002			**X**	
219	Processor Availability	"Service Level Agreements," Meta Group, 2002			**X**	
220	Voice Communications	"Service Level Agreements," Meta Group, 2002			**X**	
221	Help Desk Availability	"Service Level Agreements," Meta Group, 2002			**X**	
222	Application Processing	"Service Level Agreements," Meta Group, 2002			**X**	
223	Application Availability	"Service Level Agreements," Meta Group, 2002		**X**		
224	Help Desk Resolution	"Service Level Agreements," Meta Group, 2002		**X**		
225	Help Desk Wait Queue	"Service Level Agreements," Meta Group, 2002		**X**		
226	Customer Satisfaction	"Service Level Agreements," Meta Group, 2002		**X**		
227	Network Uptime	"Service Level Agreements," Meta Group, 2002		**X**		
228	Cost Savings	"Service Level Agreements," Meta Group, 2002	**X**			
229	Revenue Generation	"Service Level Agreements," Meta Group, 2002	**X**			

230	Process Improvements	"Service Level Agreements," Meta Group, 2002	**X**			
231	Application Availability	"Service Level Agreements," Meta Group, 2002	**X**			
232	Help Desk Resolution	"Service Level Agreements," Meta Group, 2002	**X**			

Appendix E IMMOC Objectives and Requirements

The IMMOC is an integrated element that provides a real-time network and system information and control mechanisms to ensure completion of the IMMOC maintenance mission. The IMMOC is the combination of hardware and software tools, personnel, and processes used to monitor, manage, and control the IMMOC IT architecture.

E.1 Mission:

The IMMOC will provide continuous, centralized service support and service delivery functions for the entire enterprise IT infrastructure, communications links, and network elements that support the IMMOC maintenance missions. The intent of the IMMOC is to allow for access to IMMOC central management system from any node in the maintenance chain.

The IMMOC provides a centralized IT service function for monitoring, performance analysis, fault isolation, maintenance coordination, intrusion detection, configuration management, and system administration. The IMMOC is the IT single point of contact for internal or external technicians or operations personnel.

E.2 Operations

The IMMOC will be commanded by the IMMOC Director of Maintenance Mission Operations to ensure Operational Mission accomplishment.

The IMMOC will be operated and maintained by Contractor Logistic Support (CLS) personnel and will act as the Single Point of Contact (SPOC) for IT related services and functions.

E.3 Functions

Primary System Center functions include incident management, network operations and management, performance analysis, fault resolution, maintenance coordination, configuration management, system administration, and security management.

Additionally, the IMMOC will participate in problem, change, availability, release, service continuity, service level, and capacity management functions as necessary.

Successful IMMOC mission operations are highly dependent on two main factors, infrastructure reliability, and infrastructure support.

The primary IMMOC will be located at [TBD]. Back-up locations will be located at [TBD].

E.4 Constraints

The primary capabilities for the IMMOC are extracted from and aligned with AFI 33-115, Volume 1, Network Management, which defines the required network management services for supporting critical AF communications and information networks. Additional IMMOC capabilities, roles, and responsibilities will be derived from the 15 programs System Specification requirements, customer and IMMOC Operating Instructions (OIs), and industry best practices (ITIL).

Successful IMMOC mission operations are highly dependent on two main factors, infrastructure reliability, and infrastructure support.

In order to address network and system growth, the IMMOC program will move away from the current service paradigm of localized element support and adopt a network-centric enterprise model for centralized, integrated service support and service delivery.

E.5 Requirements

E.5.1 Organizational

1. The IMMOC shall align closely with the customers' organization (civil and government), structure, and design.
2. The IMMOC shall allow for standardization of crews, positions, functions, terminology, training, and reporting with the intent of providing both immediate net-ops homogeneity and supporting larger customer initiatives in the future.

E.5.2 Architecture

3. The IMMOC architecture shall provide the following in accordance with "mission assurance" practices:

   - Centralized element for mission support functions
   - Consolidation of individual site maintenance concepts
   - Improved organizational workflow
   - Increased mission success ability
   - Risk Reduction of Mission Operations
   - Scalability of IMMOC support
   - Response to customer Initiatives
   - Operational Situational Awareness and support
   - IMMOC Systems Situational Awareness and support

E.5.3 Functional Structure

1. The IMMOC functional structure shall consist of network ops, mission systems, and ops support areas.

   - The IMMOC Network Operations element shall consist of Network Management, Event Management, and Information Assurance areas.
   - The IMMOC Mission Systems element shall consist of Network Administration, Database Management, System Administration, Event and Incident Management, and Command and Control.
   - The Operations Engineering element shall provide support to the IMMOC in the areas of configuration management, training, standardization/evaluation, engineering (system integration), planning and scheduling.

E.5.4 Contractor Logistics Support Tiered Structure

1. The IMMOC Contractor Logistics Support (CLS) shall consist of a tiered support structure to allow for readily available resources and escalating technical support.
2. The IMMOC CLS four tiers shall consist of Tier 1 – Element Technician, Tier 2 – Enterprise Specialists, Tier 3 – Engineers, and Tier 4 – Vendor / Supplier Support.

E.5.5 Mission Areas

1. The IMMOC shall execute a System Overwatch Mission
    - The IMMOC shall monitor the entire maintenance system and report to higher-headquarters and mission stakeholders the status of the maintenance system
    - The IMMOC shall execute a Network Management (S&NM**)** mission
    - The IMMOC shall execute a System Management (S&NM**)** mission
    - The IMMOC shall execute a Fault, Configuration, Accounting, Performance, and Security (FCAPS) Management mission
2. The IMMOC shall execute an Information Dissemination Management (IDM) mission
    - The IMMOC shall deliver information and coordinate with external entities in accordance with Air Force Instructions and Standard Operating Procedures.
    - The IMMOC shall deliver information and coordinate with internal entities in accordance with AFI and SOP.
3. The IMMOC shall execute a Maintenance Mission Command and Control mission

E.5.6 IMMOC Personnel

1. The IMMOC shall be staffed as a 24x7x365 entity on a shift rotation basis.
2. IMMOC staff shall be increased during the daytime to handle aperiodic operations.
3. The IMMOC crew position complement shall consist of a Crew Chief, Service Desk, Job Control, Network Management, Network Admin, and Network Defense Roles.

E.5.7 Information Exchange and Reporting

1. The IMMOC shall be able to report network status and management actions via scheduled and unscheduled reports.
2. The IMMOC shall create and disseminate the following specific reports: (REF 5.1.1)
    - Operational event/incident reports (OPREP)
    - Situation report (SITREP)
    - Information operations condition (INFOCON)
    - Time compliance network order (TCNO)
    - Command, Control, Communications, and Computers (C4) Notice to Airmen (NOTAM)
3. Perform information dissemination management
    - Implement, track, document, and report compliance with TCNOs.
    - Issue NTOs, implement, track, document, and report compliance with TCNOs.
    - Ensure two-person compliance procedures are followed according to AFI 33-138 when implementing TCNOs.
    - Issue and review all C4 NOTAMs for applicability to all theater unique information systems according to AFI 33-138.
    - Draft SITREPS according to AFI 10-206. Draft OPREPs according to AFI 10-206 to document and report significant network events affecting theater-level systems.

- Provide Service Desk services to NCCs and other NOSC customers for the theater; forward lessons learned and situations requiring additional assistance to next upper level tier Help Desk.
- Draft SITREPS according to AFI 10-206. Draft OPREP3s according to AFI 10-206 to document and report significant network events affecting base-level systems.
- Provide Service Desk services to IMMOC users and serve as focal points for network, to include IMMOC IT services, problem resolution. Forward lessons learned and situations requiring additional assistance to next upper level tier Service Desk.

E.5.8 Network Management

1. The IMMOC shall enable SNMP on all enterprise infrastructure devices, network management servers, security management servers, web proxy servers, firewalls, Domain Name Service (DNS) servers, domain controllers, Dynamic Host Configuration Protocol (DHCP) servers, and Active Directory (AD) servers.

2. The IMMOC shall ensure that Simple Network Management Protocol (SNMP) connectivity between operational elements, support elements, and external interfaces is fully functional.

3. The IMMOC shall develop and enable Access Control Lists (ACL) or other methods to prevent unauthorized read and write privileges from illicit or rogue management stations.

4. The IMMOC shall disable or remove SNMP on devices if not managed (e.g., printers, plotters, print servers, workstations)

5. The IMMOC shall ensure SNMP vulnerability scans are run monthly within the theater using vulnerability assessment tools to analyze base networks under Network Operations Security Center (NOSC) or Network Control Center (NCC) control.

6. Basic network management services:

- Network Management - provide data integrity assurance, upgrade control, and configuration management capabilities. Network Fault Resolution – provides fault detection, troubleshooting support, restoration status, and lab support.
- Network Services – provision new communications links, completes all acceptance testing, accepts service, and certifies the new service end-to-end.
- Network Performance Analysis - provides performance metrics, trend analysis, and data storage.
- Network Security Administration – provide access control and intrusion detection, and handle information assurance items such as Advisory Compliance Messages, Virus notices and bulletins.
- Interact with Defense Information Systems Agency (DISA), Joint Task Force (JTF) Global Network Operations (GNO), Theater Network Operation Security Centers (NOSC), and the commercial sector to identify and correct anomalies in IMMOC networks, systems, and applications.
- Issue NTOS as well as track, document, and report compliance with TCNOS according to AFI 33-138, directing all AF-GIG operational, security, and configuration-based changes.

- Ensure two-person compliance procedures are followed according to AFI 33-138 when implementing TCNOs.
- Issue Air Force-level Command, Control, Communications, and Computer (C4) Notice to Airmen (NOTAM) according to AFI 33-138.
- Direct all Air Force (AF) Global Information Grid (GIG) operational, security, and configuration based changes.
- Draft Situation Reports (SITREPS) according to AFI 10-206, Operational Reporting. Draft Operational Event/Incident Reports (OPREP) according to AFI 10-206 to document and report significant network events affecting Defense Information Systems Network (DISN) connections not previously reported in SITREPS.
- Utilize Network Common Operating Picture (NETCOP) to consolidate NOSC up-channeled metrics of C4 systems and report overall AF-GIG metrics to Secretary of the Air Force (SAF/XC), and other senior leaders as required.
- Monitor and report status and critical metrics of IMMOC IT services, as defined by the AF Chief Information Officer (CIO), Non-classified Internet Protocol (IP) Routed Network (NIPRNET), Secret IP Routed Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS) connections to senior leaders and theater NOSC, MSC, FAC, and base Network Command Centers (NCC) as needed or required.
- Report to JTF-GNO COMAFFOR validated NETAs, suspicious activities, and security incidents to DOD CERT, GNOSC, Air Force office of Special Investigations (AFOSI), Information Warfare Flights, theater NOSCs, NCCs, and other activities, in accordance with DOD and Air Force guidelines.

7. System and network management specifics

- Perform continuous voice, video and data network monitoring and analysis of operations for identification of network availability or degradation events.
- Ensure situational awareness of CITS equipment is maintained and respond/report any system degradation events.
- Manage IMMOC level (af.mil and af.smil.mil) DNS, naming convention for the Air Force, maintain a Name Server (NS) record for all IMMOC name servers in the af.mil zone and provide technical support for the af.mil and af.smil.mil domain and sub-domains.
- Monitor Air Force-level Internet Protocol (IP) address space.
- Manage the Tactical Internet Protocol (TAC-IP) Program to provide temporary IP address space for deployed units.
- Administer and maintain Air Force-level system capabilities as negotiated in SLAs.
- Manage the USAF Circuit Upgrade Program, identify and report circuits that exceed established thresholds to the Systems Network (AFSN) office.
- Provide and manage external DNS service to assigned bases, and internal DNS service for IT services that are consolidated, and coordinate with AFNOSC Net Operations Division on Air Force-level DNS issues.
- Manage theater-level (theater.af.mil, theater.ds.af.mil, theater.af.smil.mil, and theater.ds.af.smil.mil) DNS and assigned IP addresses. Those theater NOSCs that manage base-level IP addresses will follow guidance in the following paragraphs.

- Perform distributed control of remote access services for the theater. Follow guidance in paragraph
- Provide theater level Core Services (as defined in paragraph 6.4.) to assigned bases.
- Provide Network Time Protocol (NTP) management. NOSCS will use NTP on all systems within the CITS Network Management and Network Defense (NM/ND) boundary to synchronize system clocks with a local Global Positioning System (GPS) receiver. Additionally, ensure that as a minimum NTP is enabled on all core servers and backbone equipment.
- Detect, respond, and report network events affecting operational availability of theater network, user service levels, support to critical applications, and core services to the AFNOSC and others as appropriate.
- Provide technical assistance to assigned NCCs.
- Perform system backup and disaster recovery procedures on NOSC managed core services.
- Maintain capability to filter web sites to meet operational requirements, e.g., MINIMIZE.
- Establish local procedures for notification of MINIMIZE according to Allied Communications Publication (ACP) 121/United States Supplement (US SUP)-1, (C) Communication Instructions General (U).
- Monitor and manage Core Services via tools provided by the CITS Program Management office.
- Manage internal base DNS if not centrally managed by the theater NOSC.
- Manage all base IP address space through utilization of Dynamic Host Configuration Protocol (DHCP). DHCP will allocate dynamic IP addresses for:
- All noncritical workstations connected to the internal base network. Noncritical workstations will have a lease of 30 days applied to them; this ensures, with relative certainty that the same IP is assigned to a workstation each time a new reservation is issued. In instances where there is a documented IP address shortage for a DHCP scope (e.g., more than 80 % utilization), the lease time can be adjusted to a shorter lease duration for that particular scope so that IP addresses can be recovered more quickly.
- Remote Access Clients. The use of a remote access modem will be accomplished according to AFI 33-202, Volume 1.
- In coordination with the NOSC, provide and control all remote dial-in/dial-out communications access services. Place the communications server capable of handling dial-in and dial-out services within the CITS network battle management/network defense (NBM/ND) boundary to prevent the possibility of back-door access. This means that organizations will not connect external access devices to the base network. The NCC controls all remote dial-in/dial-out communications services. The NCC will place all remote dial-in/dial-out communications servers (remote access servers) on an alternate interface (not the internal or external interface) of the firewall. If an alternate interface is not available the remote access server will be placed off the external interface of the firewall. ANG NCC. CITS does not provide ANG NCCs with NBM/ND equipment.
- ANG purchases firewalls (CITS supported) for each NCC. The NCC controls all remote dial-in/dial-out communications services. The NCC will place all remote dial-

in/dial-out communications servers (remote access servers) on an alternate interface (not the internal or external interface) or the firewall.

- The ANG NCC will use NTP on all systems within the security boundary to synchronize system clocks with a local GPS receiver or approved DOD source. Additionally, ensure that as a minimum NTP is enabled on all core servers and backbone equipment capable of using NTP. Preferably do not allow external NTP sources through the NBM/ND boundary due to inherent security problems. However, ANG NCCs that receive NTP from their upper level ROSC may permit NTP through the firewall by exception only (e.g., IP address to IP address).
- Provide NTP management. NCCs will use NTP on all systems within the CITS NBM/ND boundary to synchronize system clocks according to NCC technical order (TO). Additionally, ensure that as a minimum NTP is enabled on all core servers and backbone equipment capable of using NTP. Do not allow external NTP sources through the NBM/ND boundary due to inherent security problems.
- Provide messaging services to base-level users [e.g., AMHS and Simple Mail Transfer Protocol (SMTP) electronic mail]. NCCs are not required to do this if the NOSC is performing these duties.
- All IMMOC users will have an E-mail address. This is a mandatory compliance issue.
- E-mail accounts will remain active and available for 60 days following a member's permanent change of station (PCS) or separation.

8. All client devices using the base wireless infrastructure will meet the requirements specified in AFI 33-202, Volume 1.

E.5.9 Functional Requirements

1. Operate 24-hours-a-day, 7-days-a-week
2. Centralized Control – provide the coordination of re-homing of communications links, call-in of essential personnel, support Job Control/Help Desk activities, coordinate communications problem resolution with external communications agencies/centers, and function as single point of contact on communications for the mission commander.
3. Provide Help Desk services to theater NOSCs as a focal point for AF-GIG problem resolution.
4. Document and track trouble calls to final resolution.
5. Supply data to program offices, DISA, JTF-GNO, and other agencies, as required, ensuring systemic Air Force-level problem areas are tracked and fixed.
6. Provide status of on-going law enforcement investigations related to computer security incidents to COMAFFOR to JTF-GNO.
7. Perform Information Assurance/Network Defense

- Perform continuous network monitoring operations for identification of on-going attacks against the network or interconnected systems.
- Provide real-time analysis, response, and reporting according to AFI 33-138 for network attacks and security incidents.
- Correlate network events with supporting network data, threat data, and technical vulnerability information.

- Maintain global situational awareness of events threatening IMMOC networks.
- Manage IMMOC long-haul user VPN.
- Maintain secure communications with NOSCs.
- Update Access Control Lists on SDP routers.
- Analyze IMMOC security posture using security management software tools such as intrusion detection and vulnerability assessment.
- Analyze customer impact of all network incidents, problems and alerts, and develop corrective actions or management changes.
- Require network defense countermeasures and other defensive or corrective actions in response to command direction, INFOCONs, or vulnerability alerts.
- Develop and/or exercise contingency plans to continue operations in at least one location in the local area and at least one location outside the local area in the event of natural or unnatural disaster, utilities failure, and contractor issues.
- Conduct NETA assessments, correlate incidents, conduct spot check compliance, and conduct on-line surveys for suspicious activities (internal and external) across IMMOC network domains. Notify COMAFFOR and the JTF-GNO of attacks and suspicious activities. Conduct trend analysis to determine patterns of attack.
- Conduct and manage IMMOC vulnerability analysis and assistance functions in accordance with AFI 33-207, Computer Security Assistance Program. Notify COMAFFOR to JTF-GNO of technical vulnerabilities impacting IMMOC computers and computer networks.
- Provide situational awareness and status to leaders at all levels based on their operational needs.
- Serve as the IMMOC single point-of-contact for receiving reports from and reporting computer security incidents and vulnerabilities to organizations external to the Air Force.
- Assist the AFNOSC (and DISA when requested through the AFNOSC) with ensuring presence of on-site personnel when requested by AFNOSC Net Operations Division to perform troubleshooting procedures to restore faulty, IMMOC owned and operated, WAN transmission equipment and circuits.
- Establish SLA, MOA, or MOU with Main Operating Bases (MOB), GSUs, tenant units, Air Force, and MAJCOM functional communities of interest defining agreed upon levels of support.
- Additionally, maintains SLA, MOA, or MOU with other NOSCs for providing back–up services as needed.
- Centrally operate and manage boundary protection and intrusion detection tools for all bases within their respective theater. This can be accomplished by either physically consolidating the servers at the NOSC or using remote management.
- Protect against unauthorized intrusions and malicious activities; monitor and report intrusion detection activity according to AFI 33-138.
- Monitor, detect, and implement NETD actions.
- Maintain secure communications with customers who require it.
- Use vulnerability assessment software tools to analyze base networks under NOSC control for potential vulnerabilities and research/recommend appropriate protective measures. Report suspected vulnerabilities and recommended protective measures to

the customers' Net Security Division. Ensure vulnerability scans are run quarterly within their theater of responsibility.

- Assists in developing a theater-level network security policy according to AFI 33-202,Volume 1.
- Provide any network reports requested by the theater IA office required for Certification and Accreditation (C&A) of theater unique systems.
- Analyze customer impact, within the theater, of all network incidents, problems and alerts, and develop corrective actions or management changes.
- Manage desktop services (paragraph 6.4.4.); consolidating services to the NOSC as best fits the operational mission.
- Any new applications and their server(s), core services, network services, or desktop services and storage requirements shall meet the intent of the server consolidation architecture using remote management, co-location or shared hosting consolidation as appropriate to the operational mission in their initial operational capability and full operational capability.
- Provide visibility of the theater network (NIPRNET and SIPRNET) to theater commanders and directors.
- Provide NCCs, within the respective theater, visibility into NOSC-managed devices for local situational awareness.
- Oversee implementation of policies, procedures, and special instructions to NCCs.
- Support deployable operations and maintain joint capabilities.
- Provide engineering guidance to plan, install, operate, and maintain base network hardware and software.
- Perform NOSC-level systems control, maintenance, and administration functions within the theater network.
- Perform Telephony Management and Voice Protection.
- Provide centralized management and administration of the enterprise-wide Enterprise Telephony Management (ETM) platform.
- Modify the active security policy (rule set) in the ETM platform as directed by higher headquarters to react to events, anomalies, and emergencies.
- Maintain trained FSAs proficient in maintaining the server's operating system and ETM platform specific software.
- Utilize platform to generate command-wide reports (as needed) and ensure real time visibility of voice networks.
- Perform all management tasks for Fault, Configuration, Accounting, Performance, and Security (FCAPS).
- Fault management tasks include but are not limited to detection, documentation and resolution of, application system faults, system detected telecommunication faults and supporting infrastructure faults.
- Configuration management tasks include but are not limited to collection, configuration and identification of technical information of the VPS and the system's infrastructure, (e.g., IPS and network IDS, firewall exceptions, Telco Trunk nomenclatures, telephone numbers and switching items, etc.)

- Accounting management tasks include but are not limited to control and maintenance of user accounts, system access passwords, telephony authorized control list (ACL) and firewall exceptions request.
- Performance management tasks include but are not limited to control, manipulation, report generation and analysis of system collected data for base, theater, and IMMOC level management decision.
- Security management tasks include but are not limited to detection, documentation, reporting, and denial of access to unauthorized telephony exploitation.
- Provide capability to automatically and continually capture, store, archive, and retrieve network topology and application traffic data for the purposes of all engineering functions listed in this document.
- Achieve full operational capability within 4 hours after notification in situations requiring increased operations tempo surge manning.
- Partner with the customer records manager to ensure records management procedures are implemented and sustained for all enterprise storage services.
- Operate 24-hours-per-day, 7-days-per-week (with either continuous manning or on-call after-hours response capability).
- Ensure presence of on-site personnel when directed by customers.
- Perform vulnerability assessments to test and validate security of networks and systems. If vulnerabilities are discovered, provide appropriate systems administrators, unit commanders, DAA, wing and theater IA offices, and AFNOSC with test results and recommendations. Report vulnerabilities found according to AFI 33-138.
- Conduct daily traffic analysis, identify and characterize incidents, and generate incident reports with Air Force approved intrusion detection tools. Investigate each item to clarify and resolve suspicious activity. Report validated suspicious activity according to AFI 33-138. The NCC does not need to perform this function if it is done at the theater NOSC. (Does not apply to ANG NCC. ANG ROSC performs this function.)
- Review AFNOSC advisories and verify systems under NCC control are protected against documented vulnerabilities.
- Notify Information Systems Security Officers (ISSO), CSAS, FSAS, and/or users when their computers have weak configurations, vulnerabilities, and when they have been accessed, exploited, or destroyed by unauthorized persons or machines.
- Put users of IMMOC computer systems, including computers connected to a network, stand-alone computers on notice that their use constitutes consent to monitoring as specified in AFI 33-219, Telecommunications Monitoring and Assessment Program (TMAP).
- Equip all servers within the CITS NBM/ND boundary with host-based intrusion detection and network security analysis and scanning tools.
- Identify weak configurations and security holes by auditing and monitoring events occurring on the network.
- Monitor and trend audit and error logs for security violations.
- Test and validate network security to establish and maintain a target baseline for IMMOC owned systems.

- Identify and secure computer systems on an affected network. Identify computers with exploited vulnerabilities.
- Provide any network reports requested by the wing IA office required for C&A of base networks and systems.
- Coordinate on all base unique System Security Certification & Accreditation packages or requests.
- Develop local procedures to report and respond to computer security and virus incidents. . Work with the customers' IA office to identify internal actions such as local reporting channels, criteria for determining who is notified, etc.
- Perform local NETD actions and respond to NOSC or AFNOSC direction.
- Analyze customer impact, within the base, of all network incidents, problems and alerts, and develop corrective actions or management changes.

8. Network Operations Requirements

- Provide a core set of office automation application support services.
- Implement software patches and security fixes as required by the SC2
- Report events not previously detected.
- In coordination with NOSC, plan, install, operate, and maintain base network hardware and software.
- Perform regular day-to-day system backup and recovery operations on IMMOC managed servers. At a minimum of once a quarter, test recovery procedures to ensure procedures are accurate and operational.
- Develop local restore and contingency operations plans from existing operations/ war plans. Validate restore plans by testing them on at least a biannual basis.
- Maintain network and facility configuration, migration, and upgrade plans.
- Perform fault management for the local base network.
- Dispatch technicians to unmanned or user and subscriber locations when required to test, troubleshoot, and restore service.
- Coordinate with job control subscribers, local and distant support agencies, and contractors to isolate faults, restore service, and make repairs.
- Ensure a trouble-call process is established.
- Provide network and small computer maintenance support to CSAS and FSAS.
- Provide technical support to FSAS and CSAS when requested and maintain an electrostatic discharge maintenance area. See TO 00-25-234, Chapter 7, for guidance.
- Perform fault isolation to the Line Replaceable Unit (LRU) and line item equipment level. Fault isolation methods include automated diagnostics and sound troubleshooting techniques.
- Perform configuration management for the local base network. Work with the functional on base for implementation of systems. Provide a database of ports, protocol, and services that are associated with a particular system.
- Prepare and update network maps and facility equipment listings.
- Establish a maintenance contract and warranty plan.
- Establish a license management program according to AFI 33-114, Software Management, to ensure authorized usage for base network software.

- Perform Information Technology (IT) Equipment Custodian (EC) duty for IMMOC equipment
- Provide assistance, when needed, and perform cryptographic equipment updates on devices under the control of the IMMOC.
- Provide network/IMMOC hardware and software installation service.
- Hardware: NCCs install and configure network servers, routers, hubs, bridges, repeaters, and servers. They test and document equipment installation acceptance testing. The ANG shall follow NOSC direction for centrally managed enterprise systems (AD, Exchange, etc).
- Software: NCCs receive and inventory network software according to AFI 33-114, test and validate new software applications and network operating systems.
- Distribute and install network software releases and updates, and assist customers with software installation and customization.
- Install and configure SMTP hosts, relays, and gateways.
- Review site license agreements and remove software from systems when no longer required or authorized. Dispose or redistribute excess software according to AFI 33-114.

E.5.10 Configuration Management

1. The IMMOC will maintain the Configuration Management Database (CMDB) for the system. This will include all associated system hardware, software, firmware, documentation, environmental factors, incident reports, (and resolutions) and change requests.

2. The CMDB will be accessed only by authorized IMMOC service personnel

3. Standard Reporting Needs (From 6.5.3.1 and 6.5.3.2 and 6.5.3.3)

- All inventory in system
- System baselines (and changes as overlays)
- Auditing reports
- Lifecycle tracking
- Change logs
- Change Report and Incident reports
- Performance indicators

Appendix F Project Management

This appendix contains artifacts from the management of the study as a project to be executed over the course of the semester.

F.1 Task Execution

The study task executed on behalf of LM IS&GS Mission and Combat Support Systems (M&CSS) Space Command and Control (SC2) occurred within the specified constraints as negotiated between the study team and the project sponsor.

F.1.1 Constraints

Constraints exist on the system under study as well as on project execution.

F.1.1.1 System Constraints

The study focused on the IT aspects of the integrated maintenance mission, not on the execution of maintenance tasks.

1. The IMMOC shall honor all security restrictions traditionally found in the USG Department of Defense (DoD) security model as defined in Executive Order 13292[24].
2. The IMMOC shall conform to the CONOP delivered to the team, herein identified as Concept of Operations, Maintenance Mission Operations Center, dated 7 March 2006.
3. The integrated maintenance mission will be funded by multiple sources and the IMMOC shall, if necessary, track funds by source and type
4. Maintenance actions performed at operational sites are distinct from depot maintenance regardless of whether the depot is physically collocated with the operational site
5. The system is an N-Tiered maintenance system in which the leaf nodes are system (operational) sites and the root nodes are termed “factories.” All other nodes are depots.
6. Factories only shift work to accommodate higher-priority work
7. Sites see the maintenance system as a single chain from the site to the factory along primary maintenance paths. Alternate paths may, or may not exist.

F.1.1.2 Study Constraints

1. No proprietary information will be provided in the execution of this project. If information cannot be provided, the team will make appropriate assumptions and document them in the study.
2. The primary tool suite is the Microsoft (MS) Office suite, including MS Word, MS PowerPoint, MS Excel, MS Visio, and MS Project.
3. SysML-based content will be delivered in native format, eXtensible Markup Language (XML) format where possible, and as images of the content embedded as needed for reference purposes.

[24] http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html

4. Deliverables will be provided in Portable Document Format (PDF) by default and in other formats as necessary. Wherever possible, the team will provide content that is compatible with the sponsor tool suite.
5. The study period of performance is bound by the course schedule.
6. No funds will be provided to the students in the execution of this task.

F.2 Contract Data Requirement List (CDRL) Deliverables

Table F.2-3: CDRLS and Delivery Dates

CDRL Number	CDRL Title	Description	Due Date
001	Proposal	• Statement of Objectives • Problem Definition • Preliminary Requirements • Approach • Expected Results • Project Plan	15 February 2007
002	Proposal Briefing	Briefing to Advisor on Project	15 February 2007
003	Weekly Status Reports	• Summary of progress this week • Summary of progress to date • Risks/Issues	Weekly
004	Draft Study	Initial draft, annotated outline	29 March 2007
005	Final Study	Final report	5 May 2007
006	Final Presentation Draft 1	Initial draft of final presentation	26 April 2007
007	Final Presentation Draft 2	Updated draft of final presentation	3 May 2007
008	Final Presentation	Final presentation	11 May 2007
009	Project Website	Website containing project data	11 May 2007

F.3 Staff Roles and Responsibilities

Table F.3-1: Project Team Members, Roles, and Responsibilities

Team Member	Role	Responsibility
David Dumont M&CSS LM IS&GS	Project Sponsor	• Primary project sponsor • Approve/reject project concept • Approve/reject project scope • Approve/reject project work products
Yolanda Lee M&CSS LM IS&GS	Project Sponsor	• Secondary project sponsor • Approve/reject project concept • Approve/reject project scope • Approve/reject project work products

Table F.3-1: Project Team Members, Roles, and Responsibilities

Team Member	Role	Responsibility
Dr. Katherine Laskey SEOR GMU	Project Advisor	• Validate project sufficiency and appropriateness • Grade progress
Joshua Icore	Project Team	• Project and schedule management • Document control and CM • Mission analysis • Sponsor Liaison
Mark Icore	Project Team	• Architecture • Data analysis • Modeling • Tool selection and training
Capt. Scott Sweeney, USAF	Project Team	• Mission analysis • Requirements analysis • Website

F.4 Period and Place of Performance

F.4.1 Period of Performance

25 January – 11 May 2007

F.4.2 Place of Performance

George Mason University, Fairfax, VA

F.5 Resources

Three (3) graduate students pursuing Masters of Science degrees in Systems Engineering from the Volganeau School of Information Technology and Engineering at GMU will execute the IMMOC study. The three students are Joshua Icore, Mark Icore, and Capt. Scott Sweeney (USAF).

The IMMOC study team will have access to the project sponsor, via email and telephone. The project sponsor is Mr. David Dumont, Lockheed Martin (LM) Information Systems and Global Services (IS&GS).

F.5.1 GMU-Provided Resources

- Rational System Developer v7 license
- WebCT Collaboration Site

F.5.2 Sponsor-Provided Resources

- Document and deliverable reviews
- Subject matter expertise

F.5.3 Student-Provided Resources

- Automated Data Processing Equipment (ADPE)
- Microsoft Office tool suite (Excel, PowerPoint, Project, Visio, Word)

F.6 Baseline Project Schedule

This section contains screen captures of the baseline Gantt chart representation of the study schedule. The screen captures show in varying levels of details milestones and task details.

F.6.1 Project Schedule Milestones

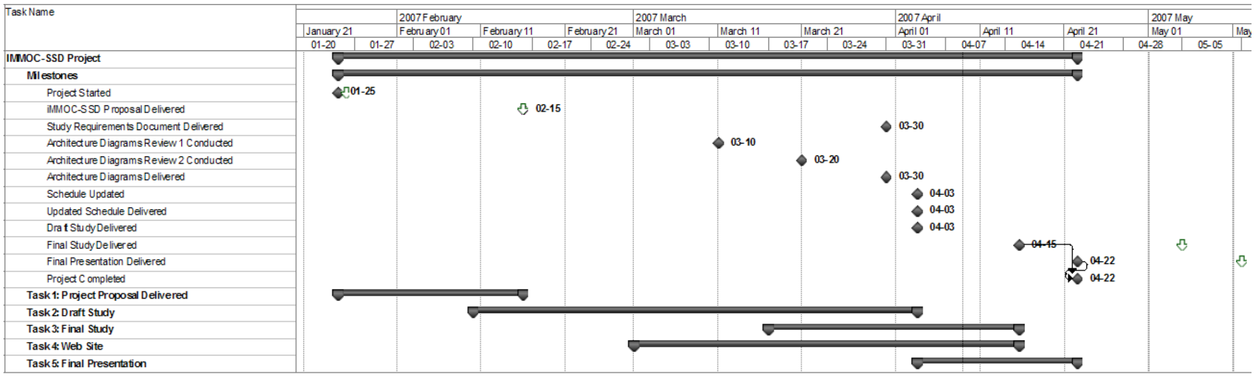
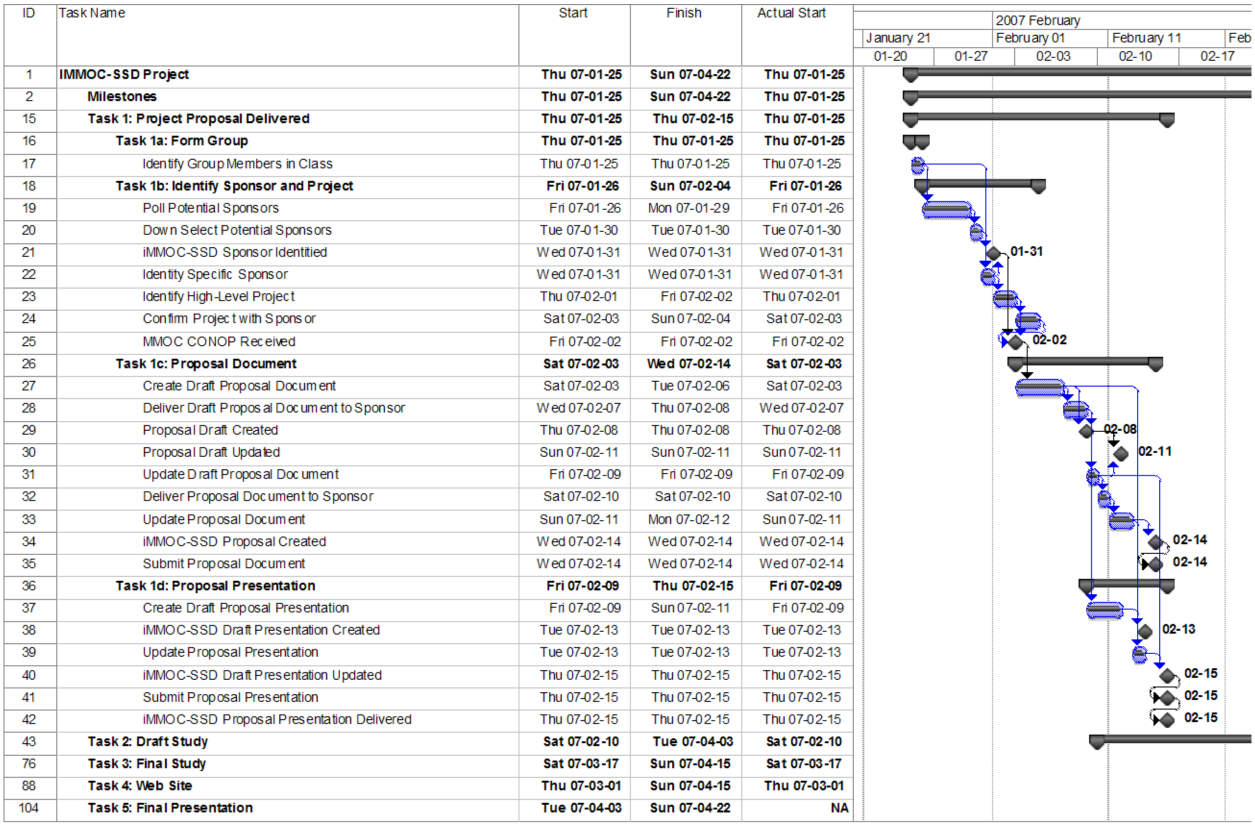


Figure F.6-1: Project Schedule – Milestone Rollup

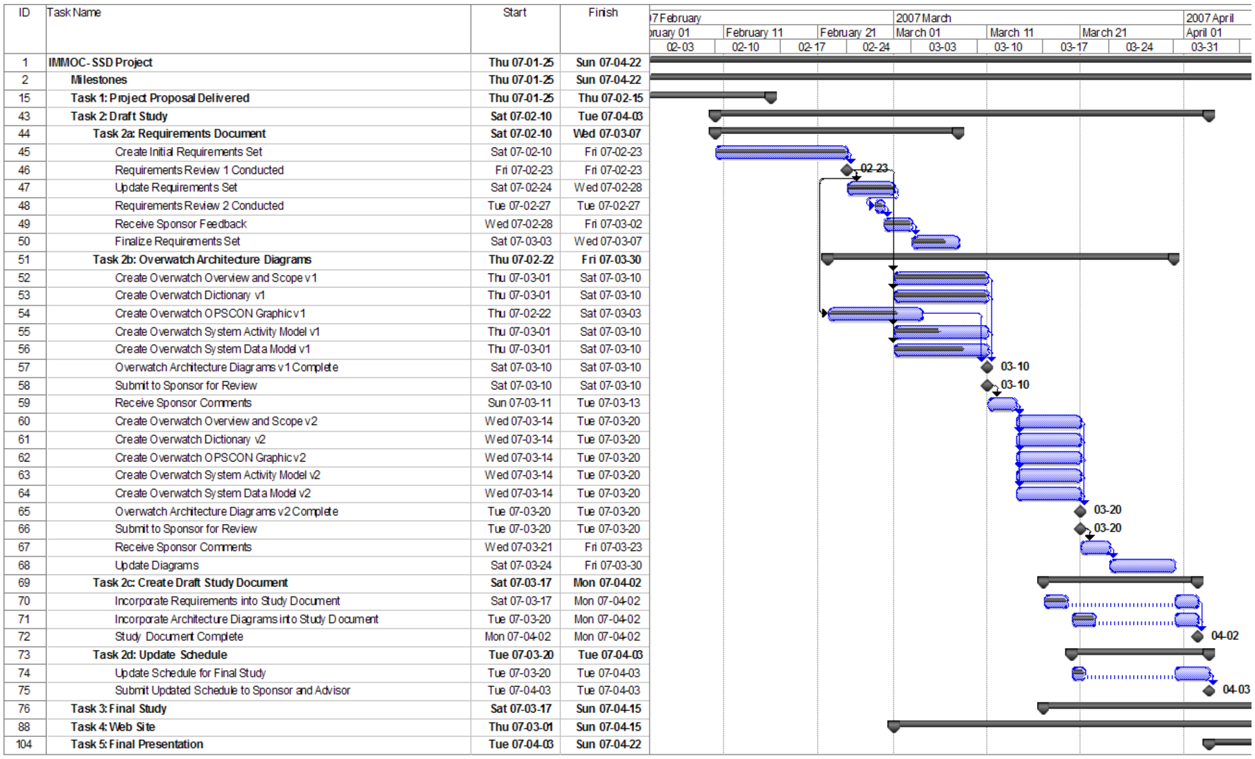
F.6.2 Task 1 Schedule



ID	Task Name	Start	Finish	Actual Start
1	**IMMOC-SSD Project**	**Thu 07-01-25**	**Sun 07-04-22**	**Thu 07-01-25**
2	**Milestones**	**Thu 07-01-25**	**Sun 07-04-22**	**Thu 07-01-25**
15	**Task 1: Project Proposal Delivered**	**Thu 07-01-25**	**Thu 07-02-15**	**Thu 07-01-25**
16	**Task 1a: Form Group**	**Thu 07-01-25**	**Thu 07-01-25**	**Thu 07-01-25**
17	Identify Group Members in Class	Thu 07-01-25	Thu 07-01-25	Thu 07-01-25
18	**Task 1b: Identify Sponsor and Project**	**Fri 07-01-26**	**Sun 07-02-04**	**Fri 07-01-26**
19	Poll Potential Sponsors	Fri 07-01-26	Mon 07-01-29	Fri 07-01-26
20	Down Select Potential Sponsors	Tue 07-01-30	Tue 07-01-30	Tue 07-01-30
21	iMMOC-SSD Sponsor Identitied	Wed 07-01-31	Wed 07-01-31	Wed 07-01-31
22	Identity Specific Sponsor	Wed 07-01-31	Wed 07-01-31	Wed 07-01-31
23	Identify High-Level Project	Thu 07-02-01	Fri 07-02-02	Thu 07-02-01
24	Confirm Project with Sponsor	Sat 07-02-03	Sun 07-02-04	Sat 07-02-03
25	MMOC CONOP Received	Fri 07-02-02	Fri 07-02-02	Fri 07-02-02
26	**Task 1c: Proposal Document**	**Sat 07-02-03**	**Wed 07-02-14**	**Sat 07-02-03**
27	Create Draft Proposal Document	Sat 07-02-03	Tue 07-02-06	Sat 07-02-03
28	Deliver Draft Proposal Document to Sponsor	Wed 07-02-07	Thu 07-02-08	Wed 07-02-07
29	Proposal Draft Created	Thu 07-02-08	Thu 07-02-08	Thu 07-02-08
30	Proposal Draft Updated	Sun 07-02-11	Sun 07-02-11	Sun 07-02-11
31	Update Draft Proposal Document	Fri 07-02-09	Fri 07-02-09	Fri 07-02-09
32	Deliver Proposal Document to Sponsor	Sat 07-02-10	Sat 07-02-10	Sat 07-02-10
33	Update Proposal Document	Sun 07-02-11	Mon 07-02-12	Sun 07-02-11
34	iMMOC-SSD Proposal Created	Wed 07-02-14	Wed 07-02-14	Wed 07-02-14
35	Submit Proposal Document	Wed 07-02-14	Wed 07-02-14	Wed 07-02-14
36	**Task 1d: Proposal Presentation**	**Fri 07-02-09**	**Thu 07-02-15**	**Fri 07-02-09**
37	Create Draft Proposal Presentation	Fri 07-02-09	Sun 07-02-11	Fri 07-02-09
38	iMMOC-SSD Draft Presentation Created	Tue 07-02-13	Tue 07-02-13	Tue 07-02-13
39	Update Proposal Presentation	Tue 07-02-13	Tue 07-02-13	Tue 07-02-13
40	iMMOC-SSD Draft Presentation Updated	Thu 07-02-15	Thu 07-02-15	Thu 07-02-15
41	Submit Proposal Presentation	Thu 07-02-15	Thu 07-02-15	Thu 07-02-15
42	iMMOC-SSD Proposal Presentation Delivered	Thu 07-02-15	Thu 07-02-15	Thu 07-02-15
43	**Task 2: Draft Study**	**Sat 07-02-10**	**Tue 07-04-03**	**Sat 07-02-10**
76	**Task 3: Final Study**	**Sat 07-03-17**	**Sun 07-04-15**	**Sat 07-03-17**
88	**Task 4: Web Site**	**Thu 07-03-01**	**Sun 07-04-15**	**Thu 07-03-01**
104	**Task 5: Final Presentation**	**Tue 07-04-03**	**Sun 07-04-22**	**NA**

Figure F.6-2: Project Schedule Details– Task 1: Project Proposal

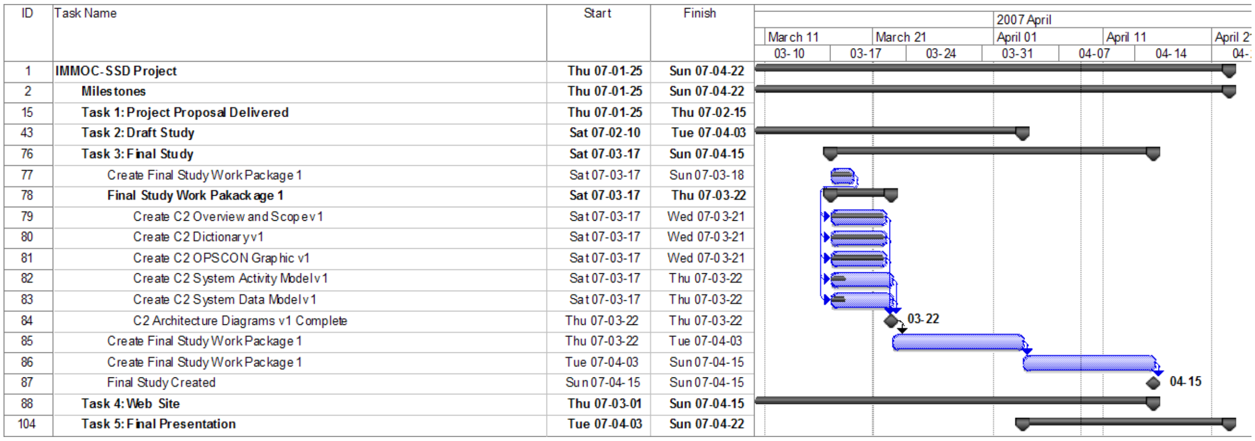
F.6.3 Task 2 Schedule



ID	Task Name	Start	Finish
1	**IMMOC-SSD Project**	**Thu 07-01-25**	**Sun 07-04-22**
2	**Milestones**	**Thu 07-01-25**	**Sun 07-04-22**
15	**Task 1: Project Proposal Delivered**	**Thu 07-01-25**	**Thu 07-02-15**
43	**Task 2: Draft Study**	**Sat 07-02-10**	**Tue 07-04-03**
44	**Task 2a: Requirements Document**	**Sat 07-02-10**	**Wed 07-03-07**
45	Create Initial Requirements Set	Sat 07-02-10	Fri 07-02-23
46	Requirements Review 1 Conducted	Fri 07-02-23	Fri 07-02-23
47	Update Requirements Set	Sat 07-02-24	Wed 07-02-28
48	Requirements Review 2 Conducted	Tue 07-02-27	Tue 07-02-27
49	Receive Sponsor Feedback	Wed 07-02-28	Fri 07-03-02
50	Finalize Requirements Set	Sat 07-03-03	Wed 07-03-07
51	**Task 2b: Overwatch Architecture Diagrams**	**Thu 07-02-22**	**Fri 07-03-30**
52	Create Overwatch Overview and Scope v1	Thu 07-03-01	Sat 07-03-10
53	Create Overwatch Dictionary v1	Thu 07-03-01	Sat 07-03-10
54	Create Overwatch OPSCON Graphic v1	Thu 07-02-22	Sat 07-03-03
55	Create Overwatch System Activity Model v1	Thu 07-03-01	Sat 07-03-10
56	Create Overwatch System Data Model v1	Thu 07-03-01	Sat 07-03-10
57	Overwatch Architecture Diagrams v1 Complete	Sat 07-03-10	Sat 07-03-10
58	Submit to Sponsor for Review	Sat 07-03-10	Sat 07-03-10
59	Receive Sponsor Comments	Sun 07-03-11	Tue 07-03-13
60	Create Overwatch Overview and Scope v2	Wed 07-03-14	Tue 07-03-20
61	Create Overwatch Dictionary v2	Wed 07-03-14	Tue 07-03-20
62	Create Overwatch OPSCON Graphic v2	Wed 07-03-14	Tue 07-03-20
63	Create Overwatch System Activity Model v2	Wed 07-03-14	Tue 07-03-20
64	Create Overwatch System Data Model v2	Wed 07-03-14	Tue 07-03-20
65	Overwatch Architecture Diagrams v2 Complete	Tue 07-03-20	Tue 07-03-20
66	Submit to Sponsor for Review	Tue 07-03-20	Tue 07-03-20
67	Receive Sponsor Comments	Wed 07-03-21	Fri 07-03-23
68	Update Diagrams	Sat 07-03-24	Fri 07-03-30
69	**Task 2c: Create Draft Study Document**	**Sat 07-03-17**	**Mon 07-04-02**
70	Incorporate Requirements into Study Document	Sat 07-03-17	Mon 07-04-02
71	Incorporate Architecture Diagrams into Study Document	Tue 07-03-20	Mon 07-04-02
72	Study Document Complete	Mon 07-04-02	Mon 07-04-02
73	**Task 2d: Update Schedule**	**Tue 07-03-20**	**Tue 07-04-03**
74	Update Schedule for Final Study	Tue 07-03-20	Tue 07-04-03
75	Submit Updated Schedule to Sponsor and Advisor	Tue 07-04-03	Tue 07-04-03
76	**Task 3: Final Study**	**Sat 07-03-17**	**Sun 07-04-15**
88	**Task 4: Web Site**	**Thu 07-03-01**	**Sun 07-04-15**
104	**Task 5: Final Presentation**	**Tue 07-04-03**	**Sun 07-04-22**

Figure F.6-3: Project Schedule Details– Task 2: Draft Study

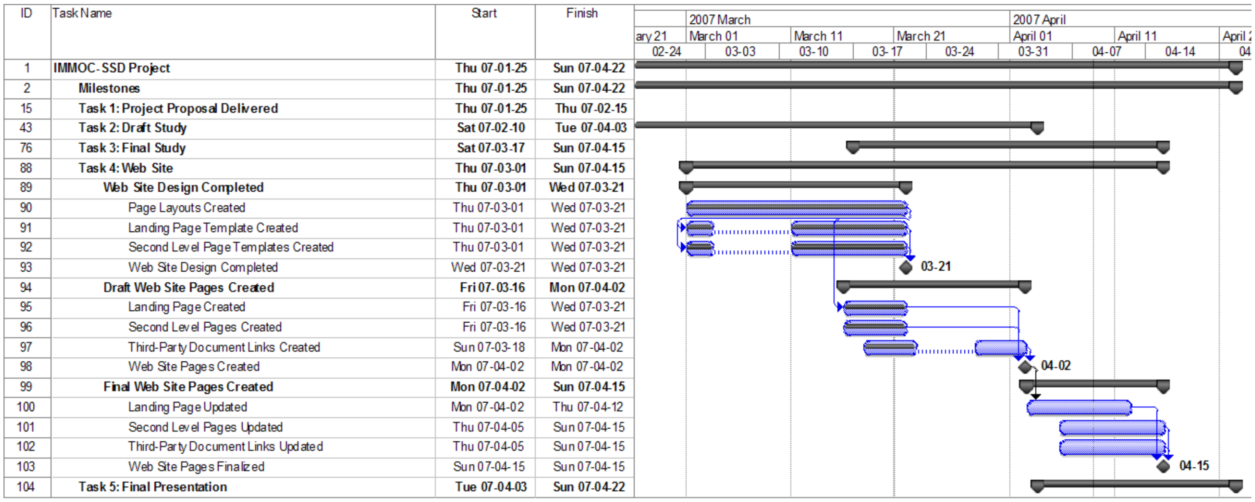
F.6.4 Task 3 Schedule



ID	Task Name	Start	Finish
1	**IMMOC-SSD Project**	**Thu 07-01-25**	**Sun 07-04-22**
2	**Milestones**	**Thu 07-01-25**	**Sun 07-04-22**
15	**Task 1: Project Proposal Delivered**	**Thu 07-01-25**	**Thu 07-02-15**
43	**Task 2: Draft Study**	**Sat 07-02-10**	**Tue 07-04-03**
76	**Task 3: Final Study**	**Sat 07-03-17**	**Sun 07-04-15**
77	Create Final Study Work Package 1	Sat 07-03-17	Sun 07-03-18
78	**Final Study Work Pakackage 1**	**Sat 07-03-17**	**Thu 07-03-22**
79	Create C2 Overview and Scope v1	Sat 07-03-17	Wed 07-03-21
80	Create C2 Dictionary v1	Sat 07-03-17	Wed 07-03-21
81	Create C2 OPSCON Graphic v1	Sat 07-03-17	Wed 07-03-21
82	Create C2 System Activity Model v1	Sat 07-03-17	Thu 07-03-22
83	Create C2 System Data Model v1	Sat 07-03-17	Thu 07-03-22
84	C2 Architecture Diagrams v1 Complete	Thu 07-03-22	Thu 07-03-22
85	Create Final Study Work Package 1	Thu 07-03-22	Tue 07-04-03
86	Create Final Study Work Package 1	Tue 07-04-03	Sun 07-04-15
87	Final Study Created	Sun 07-04-15	Sun 07-04-15
88	**Task 4: Web Site**	**Thu 07-03-01**	**Sun 07-04-15**
104	**Task 5: Final Presentation**	**Tue 07-04-03**	**Sun 07-04-22**

Figure F.6-4: Project Schedule Details – Task 3: Final Study

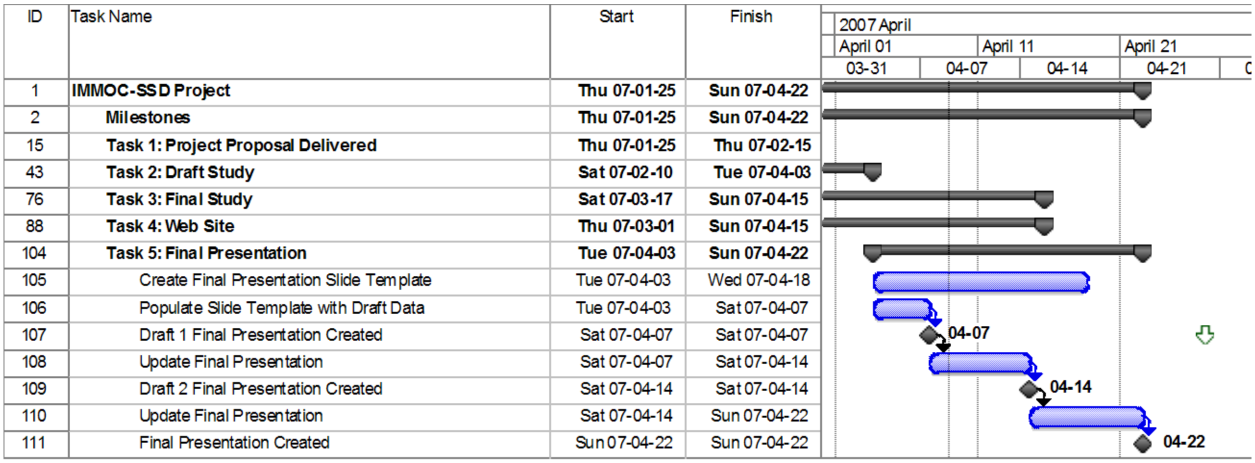
F.6.5 Task 4 Schedule



ID	Task Name	Start	Finish
1	**IMMOC-SSD Project**	**Thu 07-01-25**	**Sun 07-04-22**
2	**Milestones**	**Thu 07-01-25**	**Sun 07-04-22**
15	**Task 1: Project Proposal Delivered**	**Thu 07-01-25**	**Thu 07-02-15**
43	**Task 2: Draft Study**	**Sat 07-02-10**	**Tue 07-04-03**
76	**Task 3: Final Study**	**Sat 07-03-17**	**Sun 07-04-15**
88	**Task 4: Web Site**	**Thu 07-03-01**	**Sun 07-04-15**
89	**Web Site Design Completed**	**Thu 07-03-01**	**Wed 07-03-21**
90	Page Layouts Created	Thu 07-03-01	Wed 07-03-21
91	Landing Page Template Created	Thu 07-03-01	Wed 07-03-21
92	Second Level Page Templates Created	Thu 07-03-01	Wed 07-03-21
93	Web Site Design Completed	Wed 07-03-21	Wed 07-03-21
94	**Draft Web Site Pages Created**	**Fri 07-03-16**	**Mon 07-04-02**
95	Landing Page Created	Fri 07-03-16	Wed 07-03-21
96	Second Level Pages Created	Fri 07-03-16	Wed 07-03-21
97	Third-Party Document Links Created	Sun 07-03-18	Mon 07-04-02
98	Web Site Pages Created	Mon 07-04-02	Mon 07-04-02
99	**Final Web Site Pages Created**	**Mon 07-04-02**	**Sun 07-04-15**
100	Landing Page Updated	Mon 07-04-02	Thu 07-04-12
101	Second Level Pages Updated	Thu 07-04-05	Sun 07-04-15
102	Third-Party Document Links Updated	Thu 07-04-05	Sun 07-04-15
103	Web Site Pages Finalized	Sun 07-04-15	Sun 07-04-15
104	**Task 5: Final Presentation**	**Tue 07-04-03**	**Sun 07-04-22**

Figure F.6-5: Project Schedule Details – Task 4: Web Site

F.6.6 Task 5 Schedule



ID	Task Name	Start	Finish
1	**IMMOC-SSD Project**	**Thu 07-01-25**	**Sun 07-04-22**
2	**Milestones**	**Thu 07-01-25**	**Sun 07-04-22**
15	**Task 1: Project Proposal Delivered**	**Thu 07-01-25**	**Thu 07-02-15**
43	**Task 2: Draft Study**	**Sat 07-02-10**	**Tue 07-04-03**
76	**Task 3: Final Study**	**Sat 07-03-17**	**Sun 07-04-15**
88	**Task 4: Web Site**	**Thu 07-03-01**	**Sun 07-04-15**
104	**Task 5: Final Presentation**	**Tue 07-04-03**	**Sun 07-04-22**
105	Create Final Presentation Slide Template	Tue 07-04-03	Wed 07-04-18
106	Populate Slide Template with Draft Data	Tue 07-04-03	Sat 07-04-07
107	Draft 1 Final Presentation Created	Sat 07-04-07	Sat 07-04-07
108	Update Final Presentation	Sat 07-04-07	Sat 07-04-14
109	Draft 2 Final Presentation Created	Sat 07-04-14	Sat 07-04-14
110	Update Final Presentation	Sat 07-04-14	Sun 07-04-22
111	Final Presentation Created	Sun 07-04-22	Sun 07-04-22

Figure F.6-6: Project Schedule Details – Task 5 Final Presentation