



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE REPORT

**ONE NAVY LAB: DEVELOPING A FRAMEWORK
FOR ENHANCED COLLABORATION AND EFFICIENCY**

by

Fatou Cisse, Nithisha S. Maganahalli,
Cary F. Martinez de Andino, and Kemuel Torres-Martinez

December 2023

Advisor:

Co-Advisor:

Second Reader:

Douglas L. Van Bossuyt
Socrates Frangis, NSWC PHD
Jason Bickford, NSWC PHD

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2023	3. REPORT TYPE AND DATES COVERED Systems Engineering Capstone Report	
4. TITLE AND SUBTITLE ONE NAVY LAB: DEVELOPING A FRAMEWORK FOR ENHANCED COLLABORATION AND EFFICIENCY			5. FUNDING NUMBERS	
6. AUTHOR(S) Fatou Cisse, Nithisha S. Maganahalli, Cary F. Martinez de Andino, and Kemuel Torres-Martinez				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) Various land-based combat systems labs supporting the U.S. Navy are distributed geographically across the United States. However, a notable gap exists in the form of a land-based lab representing a fully integrated combat system of a naval vessel. Consequently, shipboard testing is the first opportunity for interoperability testing. A ship-representative land-based test site, a One Navy Lab, would support system capability development, verification and validation of technical documentation, independent verification and validation at the element and system levels, remote interface testing, and interoperability testing. However, the process of setting up the lab may entail substantial up-front costs, and currently, there is no established framework to guide decision-makers to develop such a lab. Evaluating and validating the One Navy Lab based on technical capability gains and long-term cost savings would greatly benefit decision-makers. This report develops a framework to guide stakeholder decision-making in establishing the One Navy Lab. Multiple courses of action are explored, including maintaining the status quo, building one or multiple fully integrated and geographically co-located labs, and connecting geographically distanced labs via a naval network. Following extensive research and analysis, this report concludes that maintaining the current course of action of shipboard testing is the most advantageous and cost-effective path forward.				
14. SUBJECT TERMS land-based combat systems equipment labs, shipboard environment, interoperability testing, integrated combat systems, network integration, fleet readiness, network integration framework, resource allocation, cost analysis, risk analysis, cybersecurity, land-based test site, laboratory, lab, combat systems, One Navy Lab, Naval network, NOLIN, Navy One Lab Integrated Network			15. NUMBER OF PAGES 171	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**ONE NAVY LAB: DEVELOPING A FRAMEWORK FOR ENHANCED
COLLABORATION AND EFFICIENCY**

Fatou Cisse, Nithisha S. Maganahalli, Cary F. Martinez de Andino,
and Kemuel Torres-Martinez

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Lead Editor: Nithisha S. Maganahalli

Reviewed by:

Douglas L. Van Bossuyt
Advisor

Jason Bickford
Second Reader

Socrates Frangis
Co-Advisor

Accepted by:

Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Various land-based combat systems labs supporting the U.S. Navy are distributed geographically across the United States. However, a notable gap exists in the form of a land-based lab representing a fully integrated combat system of a naval vessel. Consequently, shipboard testing is the first opportunity for interoperability testing. A ship-representative land-based test site, a One Navy Lab, would support system capability development, verification and validation of technical documentation, independent verification and validation at the element and system levels, remote interface testing, and interoperability testing. However, the process of setting up the lab may entail substantial up-front costs, and currently, there is no established framework to guide decision-makers to develop such a lab. Evaluating and validating the One Navy Lab based on technical capability gains and long-term cost savings would greatly benefit decision-makers. This report develops a framework to guide stakeholder decision-making in establishing the One Navy Lab. Multiple courses of action are explored, including maintaining the status quo, building one or multiple fully integrated and geographically co-located labs, and connecting geographically distanced labs via a naval network. Following extensive research and analysis, this report concludes that maintaining the current course of action of shipboard testing is the most advantageous and cost-effective path forward.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION AND MISSION ANALYSIS	1
A.	PROBLEM DEFINITION	3
B.	PROBLEM BACKGROUND	3
C.	RESEARCH QUESTION	5
D.	OPERATIONAL CONCEPT	6
E.	SCOPE	6
	1. Objectives.....	7
	2. Assumptions	7
	3. Constraints.....	8
F.	CAPSTONE REPORT OVERVIEW	8
II.	TEAM ORGANIZATION AND SYSTEMS ENGINEERING	
	APPROACH.....	11
A.	TEAM ORGANIZATION	11
	1. One Navy Team.....	11
	2. Team Roles and Responsibility.....	11
B.	SYSTEM ENGINEERING APPROACH.....	14
III.	BACKGROUND AND LITERATURE REVIEW	19
A.	BACKGROUND	19
	1. Joint Information Environment (JIE)	19
	2. Cybersecurity Policies	21
	3. Zones Environments	24
	4. DOD Networks	27
	5. Testing Communication and Computer Networks: An	
	Overview	29
B.	LITERATURE REVIEW	29
	1. Mission-Integrated Network Control.....	30
	2. Integrated Tactical Network.....	30
	3. Zero Trust Strategy and Roadmap	31
	4. Live Virtual Constructive.....	31
	5. Navy Center for Advanced Modeling and Simulation	32
	6. Remote Software Deployment	32
	7. Euronet Lab.....	33
	8. Implementing Engineering 2000.....	33
C.	SUMMARY	34

IV.	STAKEHOLDERS NEEDS AND REQUIREMENTS ANALYSIS	35
A.	STAKEHOLDER.....	35
B.	NEEDS ANALYSIS.....	36
C.	USE CASES.....	36
D.	REQUIREMENT ANALYSIS.....	38
V.	COURSES OF ACTIONS.....	41
A.	COA 0: ON-SHIP INTEGRATION.....	41
B.	COA 1: ONE INTEGRATED COMBAT SYSTEMS LAB.....	42
C.	COA 2: INTEGRATED COMBAT SYSTEMS LABS IN EVERY LOCATION.....	43
D.	COA 3: INTEGRATION VIA NETWORK.....	43
1.	Network Components	44
2.	Analysis of Naval Networks	49
3.	COA 3 Key Performance Parameters.....	49
VI.	MODELING AND SIMULATION	51
A.	ARCHITECTURE DESIGN.....	51
1.	Approach	52
2.	System Architectural Modeling	53
B.	NETWORK ANALYSIS.....	54
1.	Simulation Methodology	55
2.	Simulation Model.....	65
3.	Simulation Model Assumptions.....	65
4.	Simulation Analysis	71
VII.	VERIFICATION AND VALIDATION.....	77
A.	V&V ANALYSIS	77
B.	THE VALIDATION SQUARE	77
1.	Theoretical Structural Validity	79
2.	Accepting Method Consistency.....	81
3.	Empirical Structural Validity.....	84
4.	Empirical Performance Validity	87
5.	Future Validation Square Assessment.....	88
VIII.	COST AND RISK ANALYSIS.....	89
A.	COST ANALYSIS	89
1.	COA 0 Cost.....	89

2.	COA 1 Cost	90
3.	COA 2 Cost	91
4.	COA 3 Cost	92
5.	Cost Comparison	93
B.	RISK ANALYSIS.....	96
1.	Risk Management Process.....	96
2.	Risk Identification and Assessment	97
IX.	ANALYSIS SUMMARY	107
X.	CONCLUSION	113
A.	FUTURE WORK	113
1.	Additional Testing Within the DOD Network.....	114
2.	Lab Software Configuration.....	114
3.	Virtualized System Analysis.....	114
APPENDIX A: EXTENDSIM MODELING EMPIRIC TABLES AND CODE		115
EMPIRIC TABLES AND CODE.....		115
PACKET ORIGINATOR SECTION MODEL.....		121
NETWORK TRANSMISSION SECTION MODEL		122
PACKET RECEIVER FOR UDP MODEL		123
PACKET RECEIVER FOR TCP MODEL.....		124
APPENDIX B: COST ANALYSIS ASSUMPTIONS		125
APPENDIX C: COURSE OF ACTION (COA) 4		129
COA 4: INTEGRATION OF VIRTUALIZED SYSTEMS		129
COA 4: COST.....		130
COA 4: RISK AND MITIGATION STRATEGIES		131
LIST OF REFERENCES.....		135
INITIAL DISTRIBUTION LIST		143

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Scope of the Joint Information Environment (JIE) Framework. Source: Department of Defense (2019).	2
Figure 2.	One Navy Lab Operational View (OV)-1.....	6
Figure 3.	Systems Engineering “Vee” Process. Source: Walden et al. (2015).	14
Figure 4.	Mission Analysis Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).	15
Figure 5.	Stakeholder Needs and Requirement Definition Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).	15
Figure 6.	System Requirement Definition Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).	16
Figure 7.	Architecture and Design Definition Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).	16
Figure 8.	System Analysis Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).	17
Figure 9.	Integration Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).	17
Figure 10.	Verification and Validation Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).	18
Figure 11.	Risk Management Framework (RMF). Source: Open Control (n.d.).	22
Figure 12.	Department of Defense Risk Management Framework (RMF) in Acquisition Cycle. Source: Russell (2021).	24
Figure 13.	Example of Zones Architecture: Source: Defense Information System Agency [DISA] (2022).	25
Figure 14.	Integrated Tactical Network (ITN) Operational Viewpoint (OV)-1. Source: Director, Operational Test & Evaluation [DOT&E] (2020).	31
Figure 15.	One Navy Lab Use Cases	37
Figure 16.	Course of Action (COA) 0 Work on Current Land-Based Test Sites and Ships	42

Figure 17.	Course of Action (COA) 0 Architecture	42
Figure 18.	Course of Action (COA) 1 Architecture	43
Figure 19.	Course of Action (COA) 2 Architecture	43
Figure 20.	Course of Action (COA) 3 Architecture	44
Figure 21.	Department of Defense Architecture Framework (DODAF) Six-Step Process. Source: United States Department of Defense Chief Information Officer (n.d.).....	52
Figure 22.	Navy One Lab Integrated Network (NOLIN) Architecture	54
Figure 23.	Packet Originator Section.....	68
Figure 24.	Network Transmission Section.....	69
Figure 25.	Packet Receiver for User Datagram Protocol (UDP).....	70
Figure 26.	Packet Receiver for User Datagram Protocol (UDP).....	70
Figure 27.	Distance Test with Internet Service Provider (ISP) Jitter	72
Figure 28.	Distance Test with Optimal Jitters.....	73
Figure 29.	High Data Rate Test at 9700 km.....	74
Figure 30.	Validation Square. Source: Pedersen et al. (2000).....	78
Figure 31.	Method Internal Consistency Information Flow.....	82
Figure 32.	Methods to Develop Stakeholders' Recommendations.....	85
Figure 33.	Risk and Issue Management Process Overview. Source: United States Department of Defense [U.S. DOD] (2017).....	97
Figure 34.	Risk Reporting Matrix and Criteria. Source: United States Department of Defense [U.S. DOD] (2017).	98
Figure 35.	Cost vs. Benefits of the COAs	111
Figure 36.	Cost- Benefit Ratio of the COAs	111
Figure 37.	Course of Action (COA) 4 Architecture	130

LIST OF TABLES

Table 1.	Project Participants	11
Table 2.	Roles and Responsibilities of the Advisors and Stakeholders. Adapted from Bah et al. (2018)	12
Table 3.	Roles and Responsibilities of the Students. Adapted from Bah et al. (2018).....	12
Table 4.	Reviews and Their Purposes.....	18
Table 5.	Joint Information Environment (JIE) Objectives. Adapted from Department of Defense [DOD] (2019).	20
Table 6.	Stakeholders.....	35
Table 7.	High-Level Requirements.....	38
Table 8.	Low-Level Requirements.....	38
Table 9.	Real-Time Applications Latency	47
Table 10.	Network Matrix.....	49
Table 11.	Network Key Performance Parameters.....	50
Table 12.	Cost Comparison during the Implementation Year	93
Table 13.	Cost Comparison Three Years After the Implementation	94
Table 14.	Cost Comparison Six Years After the Implementation	94
Table 15.	Cost Comparison Nine Years After the Implementation.....	95
Table 16.	Course of Action (COA) 0 Risk Analysis Before Mitigation.....	99
Table 17.	Course of Action (COA) 0 Risk Analysis After Mitigation	100
Table 18.	Course of Action (COA) 1 Risk Analysis Before Mitigation.....	101
Table 19.	Course of Action (COA) 1 Risk Analysis After Mitigation	101
Table 20.	Course of Action (COA) 2 Risk Analysis Before Mitigation.....	102
Table 21.	Course of Action (COA) 2 Risk Analysis After Mitigation	102

Table 22.	Course of Action (COA) 3 Risk Analysis Before Mitigation.....	104
Table 23.	Course of Action (COA) 3 Risk Analysis After Mitigation	104
Table 24.	Evaluation of the Earned Value	107
Table 25.	Weighted Evaluation Matrix of the Courses of Action (COAs).....	110
Table 26.	ISP Probability of Packet Failure Empiric.....	115
Table 27.	ISP Jitter Probability Empiric	115
Table 28.	Course Of Action (COA) 4 Risk Analysis Before Mitigation.....	132
Table 29.	Course Of Action (COA) 4 Risk Analysis After Mitigation	133

LIST OF ACRONYMS AND ABBREVIATIONS

μs	microsecond
ACK	acknowledgement
AES	Advanced Encryption Standard
AO	Authorizing Official
ATM	asynchronous transfer mode
ATO	authorization to operate
BDP	big data platform
c	speed of light
C4	command, control, communications, and computer
CDD	capability development document
CIO	Chief Information Officer
CIWS	close-in weapon system
CMS	combat management system
CNRMA	Commander, Navy Region Mid-Atlantic
COA	course of action
CompTIA	Computing Technology Industry Association
CONOPS	concept of operations
CPU	central processing unit
CSAAC	Cyber Situational Awareness Analytic Capabilities
CSEDS	Combat Systems Engineering Development Site
D	delay
DACIS	Defense & Aerospace Competitive Intelligence Service
DARPA	Defense Advanced Research Projects Agency
DAU	Defense Acquisition University
DCOI	Data Center Optimization Initiative
DISA	Defense Information System Agency
DISN	Defense Information Systems Network

DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DODI	Department of Defense Instruction
DOT&E	Director, Operational Test and Evaluation
DREN	Defense Research and Engineering Network
ECAPS	Enterprise Collaboration and Productivity Services
EV	earned value
EW	electronic warfare
EXWC	Engineering and Expeditionary Warfare Center
FISMA	Federal Information Security Management Act
FY	fiscal year
Gb	gigabit
Gbps	gigabits per second
GHz	gigahertz
HPCMP	High Performance Computing Modernization Program
I&M	instrumentation and measurement
IATO	interim approval to operate
ICAM	Identity, Credential, and Access Management
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council on Systems Engineering
IoT	Internet of things
IP	internet protocol
IPO	input process output
IPv6	Internet Protocol version 6
ISEA	In-Service Engineering Agent
ISI	Information Sciences Institute
ISP	internet service provider
IT	information technology
ITN	Integrated Tactical Network

ITSM	information technology service management
IV&V	independent verification and validation
JIE	Joint Information Environment
JIOR	Joint Information Operations Range
JMETC	Joint Mission Environment Test Capability
JMN	JMETC MILS Network
JMS	Joint Management System
JRSS	Joint Regional Security Stack
JSN	JMETC Secret Network
Kbps	kilobits per second
kBps	kilobytes per second
km	kilometer
KPP	key performance parameters
L	length
LAN	local area network
LBTS	land-based test site
LVC	Live Virtual Constructive
M&S	modeling and simulation
Mbps	megabits per second
MBSE	model-based systems engineering
MGS	machine gun system
MILS	Multiple Independent Levels of Security
MINC	Mission-Integrated Network Control
MPE	Mission Partner Environment
MPLS	multi-protocol label switching
ms	millisecond
MSOSA	Magic Systems of Systems Architect
MTU	maximum transmission unit
MSSE	Master of Science in Systems Engineering

n	refraction index
n.d.	no date
NASA	National Aeronautics and Space Administration
NAVFAC	Naval Facilities Command
NAVSEA	Naval Sea Systems Command
NCAMS	Navy Center for Advanced Modeling and Simulation
NCTE	Navy Continuous Training Environment
NIPRNet	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOLIN	Navy One Lab Integrated Network
NPS	Naval Postgraduate School
NSWC	Naval Surface Warfare Center
OEM	original equipment manufacturer
OSI	Open Systems Interconnection
OV	operational view
PARM	program acquisition research managers
PHD	Port Hueneme Division
PM	project manager
POA&M	Plan of Action and Milestones
PV	planned value
QoS	quality of service
R&D	research and development
RDT&E	research, development, test and evaluation
RMF	risk management framework
RTT	round-trip time
SDREN	Secret Defense Research and Engineering Network
SE	systems engineering
SoS	system of systems
SSP	system security plan

STIG	security technical implementation guide
SV	schedule variance
SysML	System Modeling Language
T&E	test and evaluation
TACLANE	tactical local area network encryptor
TCP	transmission control protocol
TDM	time division multiplexed
TDY	temporary duty
TRMC	Test Resource Management Center
UC	use case
UDP	user datagram protocol
V&V	verification and validation
VLAN	virtual local area network
VPN	virtual private network
WAN	wide area network
WDM	wavelength division multiplexing

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The United States Navy requires various testing of the weapon systems, radar systems and other components that compose the shipboard combat systems. Land-based test sites (LBTS) at various Naval Sea Systems Command (NAVSEA) warfare centers and Naval contractor facilities are being used to conduct the required testing. The LBTSs “[house] equipment that can [duplicate or] simulate the operation of weapons systems” and thusly support engineers and technicians in research, development, and remote fleet support efforts (Naval Sea Systems Command [NAVSEA] n.d.). However, the LBTSs are distributed geographically across the United States and lack the representation of a fully integrated combat system. As a result, In-Service Engineering Agents use ships to perform interoperability testing, certification testing, hardware and software developmental testing, technical manual development, and training, among other responsibilities. However, it takes a significant amount of time to identify and align the ships’ schedules in preparation of the trips to complete taskings onboard. Additionally, travel costs for engineers to the ship are substantial.

This capstone report has been developed to analyze the prospective of creating a unified capability LBTS, the “One Navy Lab,” which is able to connect the separate and independent labs and enable collaboration and testing using a fully integrated platform. One Navy Lab can also be able to replicate one or more mission areas of a U.S. Naval vessel, including a representative kill chain comprised of the target sensing radar, the weapon, and the decision-making combat systems. The scope of this report is to analyze different Courses of Action (COAs) for developing a secure, reliable, and high-performance infrastructure to create a One Navy Lab, enabling users to share data, collaborate on projects, and access resources in a secure and efficient manner.

Four COAs are identified based on the stakeholders’ needs. COA 0 is to keep the current set-up and the engineers will continue to travel to utilize ships or existing labs for testing. COA 1 is to build one fully integrated combat systems lab that will be shared among the different warfare centers. For COA 2, each warfare center will have their own fully integrated combat systems labs. COA 3 will connect the separate and independent

labs using a naval network. The Department of Defense (DOD) cybersecurity requirements that must be incorporated throughout the life cycles of the COAs are also identified. One major cybersecurity requirement that COA 1, COA 2, and COA 3 have in common is each must obtain an Authorization to Operate (ATO). An ATO is a decision by a senior government official that authorizes an agency to operate an information system on their behalf.

COA 1 and COA 2 are set up in the same configuration as COA 0, thus they are all assumed to meet the interface requirements as COA 0 does. As COA 3 is a new system that has not been verified yet, it requires further analysis to determine if it meets the requirements. An analysis of COA 3's system architectures was conducted to understand the interfaces between the subsystems in order to determine the readiness level of the system and to identify its physical limitations. A simulation model was developed to evaluate the behavior of COA 3 under specific circumstances. The simulation results show that the distance between labs, jitter, and network probability of failure significantly impact packet latency, potentially causing the latency to exceed the 150 milliseconds requirement.

To support COA 3, a Naval network will need to be implemented in each warfare center taking part in the One Navy Lab. When deciding on which network best suits the One Navy Lab, this report considers bandwidth, latency, jitters, security, and availability. An investigation of existing DOD networks was conducted and the most advantageous options for COA 3 were identified. The networks identified are Joint Information Operations Range, Joint Mission Environment Test Capability Multiple Independent Levels of Security Network, Joint Mission Environment Test Capability Secret Network, Defense Research and Engineering Network, and Secret Defense Research and Engineering Network.

A cost analysis was performed to estimate the cost of the various COAs. COA 0 has a recurring cost from traveling to different locations for work (also known as temporary duty (TDY)) to complete the assignment. COA 1 has an initial cost for the set-up of one fully integrated lab and obtaining an ATO, in addition to a recurring cost from TDY to the lab and maintaining the ATO. COA 2 has an initial cost for the set-up of four fully integrated labs and getting ATOs for the labs, in addition to a recurring cost of maintaining

the ATO. As most of the networks that COA 3 has the option to use incur no network equipment and maintenance costs (as they are covered by an external agency), COA 3 has a standard life-cycle cost of obtaining and sustaining an ATO. If all four warfare centers implement the same COA, using the cost of COA 0 as a baseline and the initial cost of the COAs, it is determined that it would take 198 years for COA 1 to break even, 788 years for COA 2 to break even, and three years for COA 3 to break even. Based on the assumption of a yearly budget for LBTS incremental expansion constrained to \$6 million, it would take 20 years and 81 years to implement COA 1 and COA 2, respectively. COA 3 would be implemented in one year. As a combat system is assumed to have a five-year lifespan before requiring modernization, any COA that takes longer than five years to implement is assumed to have failed to meet requirements.

A risk analysis was also conducted to identify the risks of each COA and provide mitigation strategies for the identified risks. Each COA has its own set of risks that must be considered when utilizing them. COA 0 and COA 1 have the highest risks due to the dependency on the schedule availability of the ships and labs or the integrated lab, respectively, which can be lowered to a moderate level by utilizing the identified mitigation plans, such as: planning accordingly, constantly verifying the schedule of the ship or lab, and clearly communicating the schedule to the users. The rest of the COAs have low to moderate risks that can be lowered by implementing the proposed mitigation plans.

All evaluated COAs meet the requirements to perform the required use cases. However, this report recommends continuing to implement COA 0. COA 0 provides more value, based on the evaluation of the COAs, with respect to the evaluation measures such as time to implement the COAs, earned value, technical feasibility, scheduling risk, and other risks. Additionally, COA 0 has the lowest cost compared to the other COAs. The report concludes with the identification of several areas for future work, including additional simulations and testing using information and values consistent with the DOD network and the lab-specific hardware to confirm the accuracy of the simulation; the values and detailed network information were unable to be incorporated in this report due to their classification levels being outside of Distribution A. It is also recommended to explore the

possibility of implementing lab-specific software that is more tolerant for COA 3, and a virtualized system as a fourth alternative.

References

Naval Sea Systems Command. n.d. “Warfare Centers NSWC Port Hueneme Division: Surface Warfare Engineering Facility.” <https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Port-Hueneme/What-We-Do/Test-Evaluation/SWEF/>.

ACKNOWLEDGMENTS

One Navy Team would like to express great appreciation to all of those who assisted in the successful completion of this capstone project.

Special thanks go to our Naval Postgraduate School capstone advisor, Dr. Douglas Van Bossuyt, and our advisors and second reader from the Naval Surface Warfare Center Port Hueneme Division, Socrates Frangis and Jason Bickford. Their mentorship and limitless guidance, insights, and support were crucial over the course of the capstone project. We extend our thanks to NPS, and more specifically, the systems engineering professors through our postgraduate studies.

The successful completion of our capstone project was a collaborative effort that would not have been possible without the dedication and contributions of an exceptional team. We extend our appreciation to our fellow teammates.

Lastly, we express heartfelt gratitude to our loved ones, family, and friends for their unwavering and enduring support throughout the challenging journey of attaining our Master of Science in Systems Engineering degrees. Their countless sacrifices and endless patience during this time allowed us the opportunity to invest the time and effort needed to push through to success.

With sincere gratitude,
One Navy Team

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND MISSION ANALYSIS

Military entities such as the Navy must be agile and competitive as modern warfare undergoes rapid and accelerating evolution. It is imperative that the Navy revolutionizes its laboratory infrastructure to remain competitive in this dynamic environment. The Department of Defense (DOD) Chief Information Officer's (CIO) response to this changing environment is to create "a more secure, coordinated, seamless, transparent, and cost-effective IT [information technology] architecture" (Department of Defense [DOD] 2019, 4). To accomplish their vision, the DOD CIO has endorsed the Joint Information Environment (JIE). JIE is a framework to "improve mission effectiveness, increase cybersecurity, improve interoperability, deliver capabilities faster, and realize IT efficiencies" (DOD 2019, 35). The efforts in this report align with the JIE objectives.

To promote efficiency and innovation in the production of cutting-edge technologies, it is imperative to consider the implementation of an enterprise-style network, as seen in Figure 1. The Navy needs a network of this magnitude not only to remain competitive in the rapidly changing warfare environment, but also to maintain its strategic advantage. Technology is not the only factor affecting this shift, it is also about revolutionizing processes within the Navy. This contributes to the DOD CIO's overall goal, which is to complete the department's missions more effectively and efficiently.

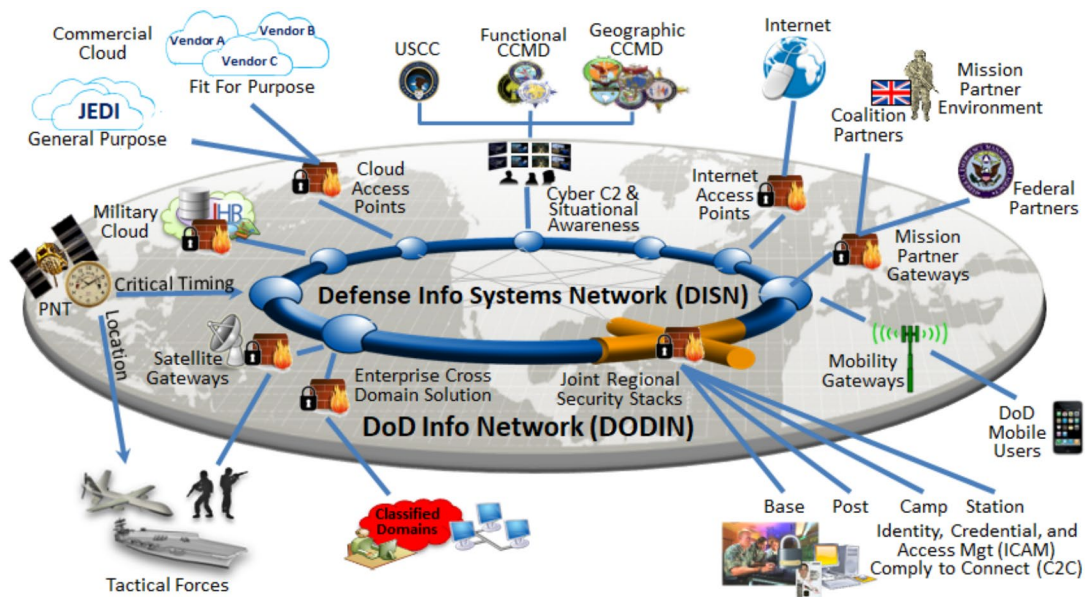


Figure 1. Scope of the Joint Information Environment (JIE) Framework.
Source: Department of Defense (2019).

This report has been developed to analyze the approach of creating a unified capability land-based test site (LBTS), or sites, to support Naval engineers and technicians in their tasks. The LBTS will be able to replicate one or more mission areas of a U.S. Naval vessel, such as a mission’s operational kill chain using the target sensing radar, the weapon, and the decision-making combat system. The developers of this report, the One Navy Team, have been tasked by the Naval Surface Warfare Center (NSWC), Port Hueneme Division (PHD) to create a framework for the evaluation of alternative ship representative LBTS configurations, which has been dubbed the “One Navy Lab.” An LBTS as such would enable engineers and technicians from different surface warfare centers in various geographical locations to collaborate on one integrated system and support each other for a successful fielding of their respective systems on the naval vessels. This report proposes methods for lab integration, documents the changes required, and analyzes integration costs, risks, and cybersecurity impacts. Mitigation strategies for cost, risk, or cybersecurity issues are also provided for the stakeholders to utilize for decision-making.

A. PROBLEM DEFINITION

The U.S. Navy's current LBTs are composed of various combat systems labs that are distributed geographically across the United States. The LBTs house "equipment that can [duplicate or] simulate the operation of weapons systems" and thusly support engineers and technicians in research, development, and remote fleet support efforts (Naval Sea Systems Command [NAVSEA] n.d.b.). However, there is an absence of a land-based shipboard environment representing a fully integrated combat system. As a result, shipboard testing is the first opportunity for interoperability testing. Connecting the many separate and independent labs will result in the desired shipboard representative system capable of supporting integrated capability development, verification and validation (V&V) of technical documentation, interoperability testing, independent verification and validation (IV&V) at the element and system level, and remote interface testing.

However, interconnection and integration can involve substantial up-front costs, and there is currently no established framework to support integration decisions. The use of a rigorous systems engineering methodology to evaluate and validate lab integration based on technical capability gains and long-term cost savings would greatly benefit the decision makers. Additionally, having a framework that can be applied to future integration efforts would significantly enhance the U.S. Navy's development and sustainability efforts.

B. PROBLEM BACKGROUND

The Naval Sea Systems Command (NAVSEA) warfare centers "work with the [Fleet] to understand their operational needs and translate them into requirements" for engineers to develop into systems or system of systems (SoS) for the naval warships (Naval Sea Systems Command [NAVSEA] n.d.c.). NSWC PHD is one of the U.S. Navy's key sources for fleet readiness as the In-Service Engineering Agents (ISEA) for combat, weapon, and radar systems. NAVSEA describes In-Service Engineering as "a very broad function that includes the installation of systems on ships, certification that the systems perform as designed, and the training and qualification of the Sailors that operate and maintain the systems" (Naval Sea Systems Command [NAVSEA] n.d.a.). To meet current mission requirements, NSWCs' ISEA periodically go aboard ships to perform certification

testing, hardware and software developmental testing, technical manual development, and training, among other responsibilities. It takes months to prepare for the organization and collaboration of ships and system elements to support the ISEA taskings. Moreover, this approach is dependent on ships' schedules and availabilities. Additionally, travel costs for the NSWC engineers are also substantial.

To help reduce associated costs and the impacts on ships' schedules, the U.S. Navy utilizes land-based labs located around the United States. These land-based labs consist of various sensor labs, weapons labs, and combat management system (CMS) labs that are, currently, limited to supporting their own systems in a localized working domain. As a result, the U.S. Navy's fleet support efforts have been hindered by the labs' localized domains by necessitating equipment redundancies and, consequently, increased scheduling and budgeting inefficiencies; multiple labs with the same equipment must be set up to fulfill the fleet support requirements, which adds additional up-front and sustainment costs. Additionally, sharing the labs with multiple efforts at the same time results in scheduling conflicts and increased budget.

The biggest hindrance these distributed labs present is the constraint on the engineers and technicians to the use of a non-integrated lab, resulting in the following limitations:

- For test and evaluation – this limits the full capacity of interoperability testing that can be conducted to resolve issues.
- For technical documentation development – this may impact the schedule as the developers may need to share lab resources with other tasks or wait for the system to be installed on the ship to finalize the technical documents.
- For hardware and software development – this means delays to schedules of elemental or combat systems certification, and as a result delays to schedules of fielding of following ships will be incurred as discrepancies are found at a later stage.

- For system installation – this means problems during installation and check-out due to possible integration incompatibility.
- For training – this means an increase in costs incurred or delays in schedule, as trainers and users may need to travel to different locations to be trained on each different system or are limited to shared lab spaces upon which the schedule is dependent.
- For fleet support – this brings system interface limitations when troubleshooting and providing technical assistance to ship force.

By establishing an LBTS of integrated combat systems, these concerns for the U.S. Navy could be mitigated.

C. RESEARCH QUESTION

This report addresses the question: is One Navy Lab a more advantageous alternative to the current set-up of shipboard testing or the non-integrated and geographically distributed labs? The following research questions have been identified to help answer the question and assist in determining if the integration of naval labs is a viable and cost-effective strategy for delivering quality products efficiently to the Fleet:

1. What are the cybersecurity standards and requirements for enclaved labs and labs that are integrated into a network?
2. What are the costs associated with different courses of action (COAs)?
3. What are the risks associated with implementing the different COAs?
4. What benefits are gained from integrating naval labs?
5. What are the limitations associated with integration of naval labs?
6. Are existing naval research and development (R&D) networks capable of supporting required interfaces?

D. OPERATIONAL CONCEPT

One Navy Lab is the concept of collaboration between different naval systems labs around the nation to streamline and optimize the testing, training, software development, hardware development, and technical documentation creation processes across multiple laboratories, as presented in Figure 2. The One Navy Lab is envisioned to enable seamless collaboration and knowledge sharing among different teams and NSWCs, enhance efficiency, and ensure consistent quality across all aspects of acquisition life cycle development.

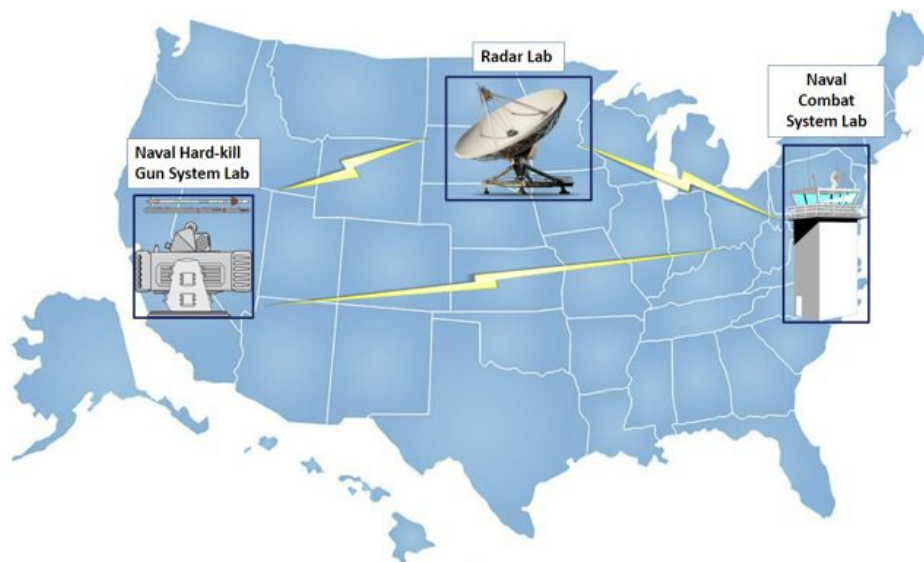


Figure 2. One Navy Lab Operational View (OV)-1

E. SCOPE

This report analyzes the One Navy Lab concept and researches the requirements for such a unified lab so that an informed decision can be made on whether to create the LBTS. The project scope is to analyze the different courses for developing a secure, reliable, and high-performance infrastructure that connects Navy laboratories and research facilities, enabling them to share data, collaborate on projects, and access resources in a secure and efficient manner. This project follows the systems engineering process to define NAVSEA requirements for the One Navy Lab. The report documents lab usage

requirements, cybersecurity requirements, installation requirements, and cost and risk involved, while developing the concept of operations (CONOPS), concept of employment, use case diagrams, Plan of Action and Milestones (POA&M), and other systems engineering artifacts. Simulation opportunities include network infrastructure, bandwidth and latency modelling, and other supporting structures.

1. Objectives

To achieve the project's goal, the following objectives were established:

- Develop a framework to enable the use of a land-based combat system environment.
- Develop a framework for evaluation of course of actions that support interoperability of naval systems.
- Determine the risks and costs associated with linking distributed labs.
- Determine the capabilities gained from the various COAs.

2. Assumptions

The following assumptions were made by the Team:

- Existing labs have already been granted authorization to operate in an enclaved lab environment.
- If an enclaved lab is to be expanded with a network, authorization to operate will be granted.
- Collaboration resources, such as personnel and technology, are available.
- The feasibility of the project will be evaluated based on the current state of technology.
- Only networks related to the DOD will be considered.

- In the integration process, other naval facilities are willing to collaborate and cooperate with PHD.
- Systems being integrated are compatible with one another.

3. Constraints

The following constraints were identified by the Team:

- Actual performance parameters are not used within the study due to the desire to keep classification level as required for public release.
- Validation of the simulation cannot be performed using DOD networks.
- The project will design a system limited to the incorporation of at least a weapons lab, sensor lab, or a combat system lab.

F. CAPSTONE REPORT OVERVIEW

There are nine chapters in this capstone report. Chapter I provides an overview of NSWC PHD and its current state, beginning with a description of its objectives and responsibilities. Additionally, the chapter discusses and elaborates on the current capability gap that NSWC faces and presents the project objectives. Chapter II discusses the One Navy Team and the advisors' organization, and their respective responsibilities. The chapter also details the systems engineering approach the team chooses to follow. In Chapter III, the team explores literature reviews conducted as background and preliminary research to learn of other similar or relevant projects. Chapter IV identifies the stakeholders, examines the functional requirements determined by analyzing the stakeholder needs, and breaks the functional requirements down into system requirements. Chapter V describes the COAs and the defined key performance parameters (KPPs). Chapter VI details the architecture of the system. The architecture will enable the system design to be traced back to each requirement. To demonstrate if the system will meet the requirements, the team details the simulation model and analyzes the results obtained from it. The V&V of the report, to verify and validate the processes to develop, model, evaluate, and analyze the One Navy Lab alternatives, is completed in Chapter VII. Chapter VIII

covers the cost and risk analyses of the COAs. Chapter IX provides the analysis of the data obtained in the chapters prior to it and a final recommendation. Chapter X concludes the capstone and identifies any future work suggested.

THIS PAGE INTENTIONALLY LEFT BLANK

II. TEAM ORGANIZATION AND SYSTEMS ENGINEERING APPROACH

The One Navy Team has been formed by Naval Postgraduate School (NPS) to research the approach for making a unified capability lab in support of Naval engineering and technician taskings. The team consists of four engineers of various educational and career backgrounds who are pursuing their Master of Science in Systems Engineering (MSSE) at NPS. This report is a capstone project that culminates the team's educational journey. The team works with their advisors to receive guidance to complete the report. The team follows the Vee systems engineering (SE) model to construct and develop this report.

A. TEAM ORGANIZATION

The following introduces the participants of the One Navy Team, advisors, sponsors and their roles in this capstone project.

1. One Navy Team

Project participants are engineers from NAVSEA NSWC PHD and the Naval Facilities Command (NAVFAC) Engineering and Expeditionary Warfare Center (EXWC). Table 1 provides the list of participants and their respective organization.

Table 1. Project Participants

Participant	Organization
Fatou Cisse	NAVFAC EXWC, Chemical Engineer
Nithisha Maganahalli	NAVSEA NSWC PHD, Mechanical Engineer
Cary Martinez de Andino	NAVSEA NSWC PHD, Mechanical Engineer
Kemuel Torres-Martinez	NAVSEA NSWC PHD, Electrical Engineer

2. Team Roles and Responsibility

The team is composed of four MSSE students. As seen in Table 2, an advisor, a co-advisor, and a second reader are assigned to guide the team. The primary stakeholders

provide invaluable insight into the capstone project topic. To ensure successful completion of the capstone project, each role, described in Table 3, has been assigned to a team member.

Table 2. Roles and Responsibilities of the Advisors and Stakeholders. Adapted from Bah et al. (2018)

Role	Members	Responsibility
Advisor	Dr. Douglas Van Bossuyt	Project advisor is responsible for providing expert advice to the team. The advisor is responsible for guiding the team to ensure the project stays on track. They provide recommendations, perform internal reviews of documentation, and answer any questions throughout the project.
Co-Advisor	Socrates Frangis	Project co-advisor is responsible for advising the team on the project as well as guiding the team to ensure the project stays on track. They provide recommendations, perform internal reviews of documentation, and answer any questions throughout the project.
Vision Owners	Richard Watanabe, Craig Tenhoff, Matthew Cole	The vision owners are responsible for guiding the team to define the scope of the project. Additionally, the vision owners are the subject matter experts on the project.
Second Reader	Jason Bickford	The second reader is responsible for reading the final drafts of the documentation for appropriate content and methodology.

Table 3. Roles and Responsibilities of the Students. Adapted from Bah et al. (2018)

Role	Member	Responsibility
Project Manager	Cary Martinez de Andino	The project manager (PM) is responsible for leading the team throughout the course of the project by keeping the team on track to meet deliverable dates. The PM is the primary liaison between the team and the stakeholders. Additionally, the PM maintains meeting notes, the schedule, and informs the team of any changes.
Deputy Project Manager	Nithisha Maganahalli	The deputy PM will act as an executive officer for the program and assist the PM as needed.

Role	Member	Responsibility
Systems Engineer	Cary Martinez de Andino	The systems engineer is responsible for overseeing the technical and engineering aspects of the project. In addition, the systems engineer is responsible for researching potentially applicable solutions/products and providing technical assistance and backup for the systems architect, test engineer, and risk/cost analyst.
Systems Architect	Kemuel Torres-Martinez	The systems architect is responsible for overseeing the development of required project architecture, and the definition of the operational needs.
Editor	Nithisha Maganahalli	The editor is responsible for reviewing the various team developed documents to maintain continuity of voice throughout and check for errors.
Configuration Management	Nithisha Maganahalli	The configuration management lead is responsible for tracking any version changes of the documents. Additionally, they are responsible for maintaining the backups of all the documents.
Research	Cary Martinez de Andino	The lead researcher is responsible for finding, maintaining, and organizing all research documents.
Test Engineer	Fatou Cisse	The test engineer oversees the development of testing necessary for validation and verification of the model.
Modeling & Simulation	Kemuel Torres-Martinez	The modeling and simulation (M&S) lead is responsible for overseeing all M&S projects. The M&S lead will be responsible for delegating tasks and ensuring the task matches the individual's capabilities.
Modeling & Simulation Team	Team	The team is responsible for performing and coordinating the modeling and simulation parts of the project.
Requirements Management	Kemuel Torres-Martinez	The requirements management lead oversees the requirements development plan and monitors any requirement changes. The requirements management lead also keeps a record of the requirement matrix.
Risk & Cost Analyst	Fatou Cisse	The risk and cost analysis lead is responsible for overseeing the development of cost estimates and risk management plan.
Procedure Development	Fatou Cisse	The procedure development lead is responsible for developing new procedures as well as monitoring existing procedures of the project.

B. SYSTEM ENGINEERING APPROACH

One Navy Team established the systems engineering approach for this capstone project. The capstone project uses the Vee Model as the SE process. The team chose this process as “its core involves a sequential progression of plans, specifications, and products,” and approaches the sequential progression in an iterative manner (Systems Engineering Department n.d., 4). The model’s process “emphasizes requirements-driven design” (Systems Engineering Department n.d., 4). Figure 3 shows the Vee model and the descriptions of the sequential key SE processes of the system life cycle.

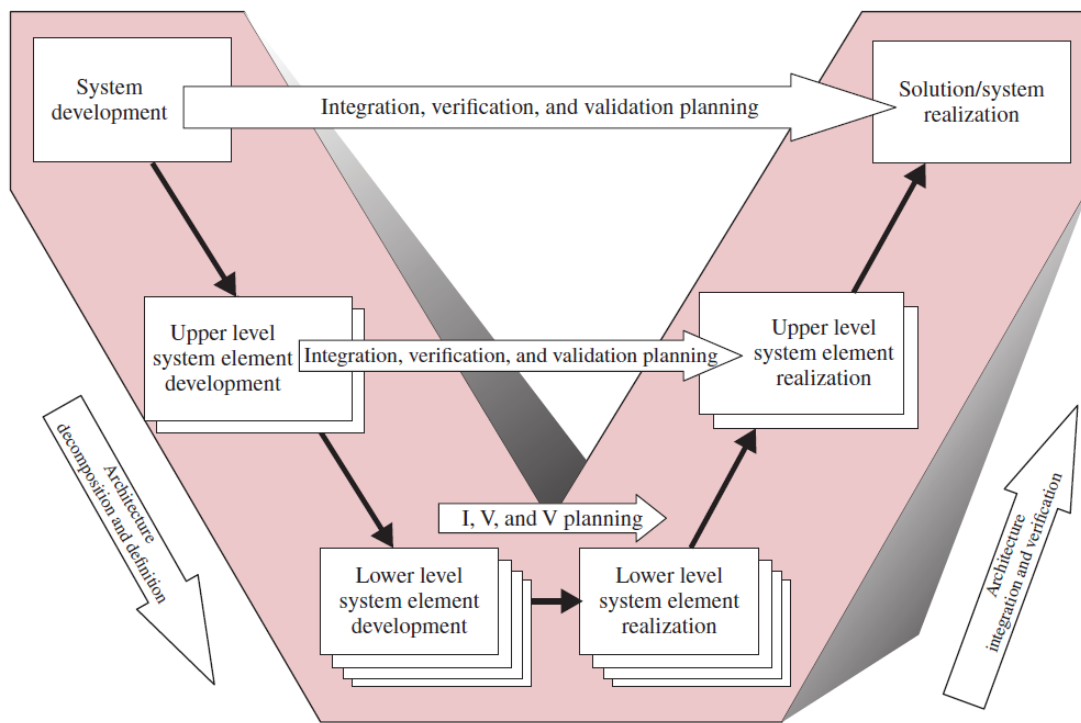


Figure 3. Systems Engineering “Vee” Process. Source: Walden et al. (2015).

Following the technical processes described in Chapter IV of the International Council on Systems Engineering (INCOSE) handbook, the capstone project starts with Mission Analysis, followed by Stakeholders’ Needs and Requirements Definition, System Requirement Definition, Architecture and Design Definition, System Analysis, Integration, and ends with Verification and Validation (Walden et al. 2015, 48–49).

As an initial step of the system life cycle, the Mission Analysis Input Process Output (IPO) Diagram shown in Figure 4 addresses the process of defining the problem and identifying possible solutions. This process also includes identifying the stakeholders and determining the operating conditions and constraints of the systems.

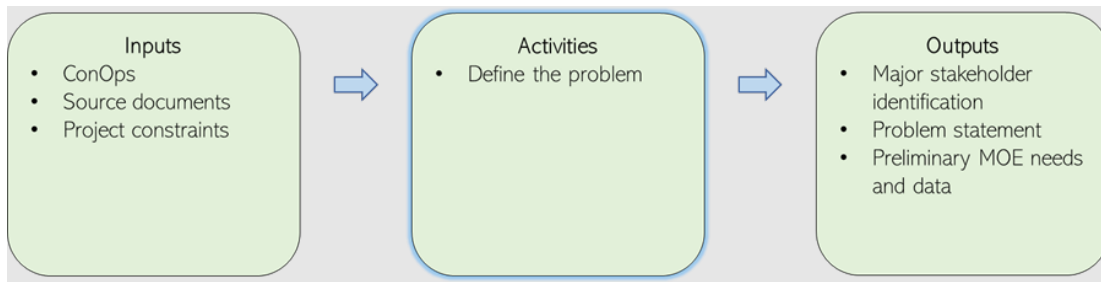


Figure 4. Mission Analysis Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).

During the Stakeholder Needs and Requirement Definition Process, shown in Figure 5, the team defines the stakeholders' needs and transforms the needs into requirements. The requirements specify the system's capabilities and its life cycle concepts.

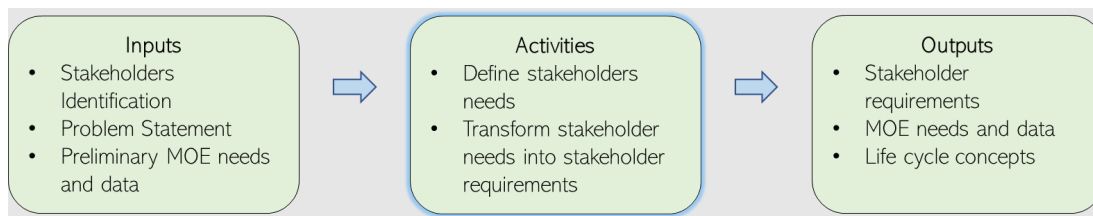


Figure 5. Stakeholder Needs and Requirement Definition Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).

The System Requirement Definition Process, shown in Figure 6, addresses the sequence of transforming the stakeholders' requirements into system requirements that meet the operational needs of the system.

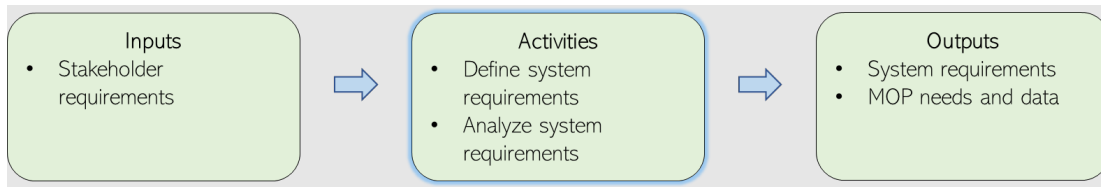


Figure 6. System Requirement Definition Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).

The Architecture Definition Process addresses the process of using the system requirements to identify and analyze possible alternatives and to select the alternative(s) that satisfy the system requirements. The Design Definition Process addresses the process of generating details on the system, enabling a consistent implementation of the final product. The Architect Definition and Design Definition Processes, shown in Figure 7, generate the system design description, interface definition, and system element descriptions, which are used to identify the optimum system that satisfies the system requirements.

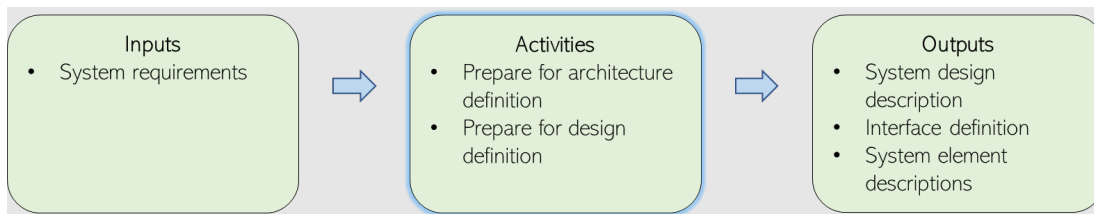


Figure 7. Architecture and Design Definition Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).

The System Analysis Process, shown in Figure 8, addresses the process of developing strong and well analyzed data to facilitate decision making. The analysis usually includes cost, risks, suitability, among others.

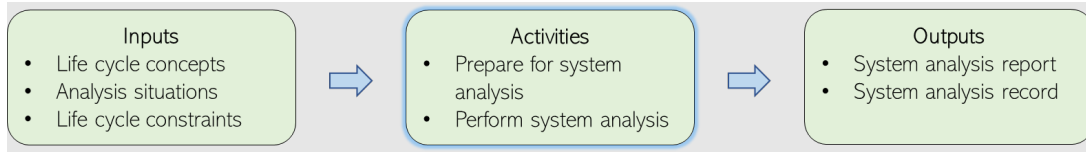


Figure 8. System Analysis Process Input Process Output (IPO) Diagram.
Adapted from Walden et al. (2015).

The Integration Process, shown in Figure 9, addresses the process of combining sets of systems elements, including hardware, software, into a unified system that meets the system, architecture, and design requirements. The correctness of the interfaces is also verified at this stage. This process would be conducted in future work when the One Navy Lab system is being constructed.

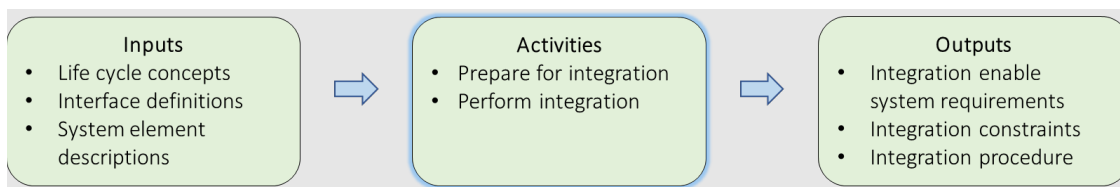


Figure 9. Integration Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).

The V&V Process, shown in Figure 10, addresses the process of testing and obtaining evidence that the system meets the requirements. It enables the user to check if the system has any errors or defects. The V&V process will be completed in future work after the One Navy Lab system has been made.

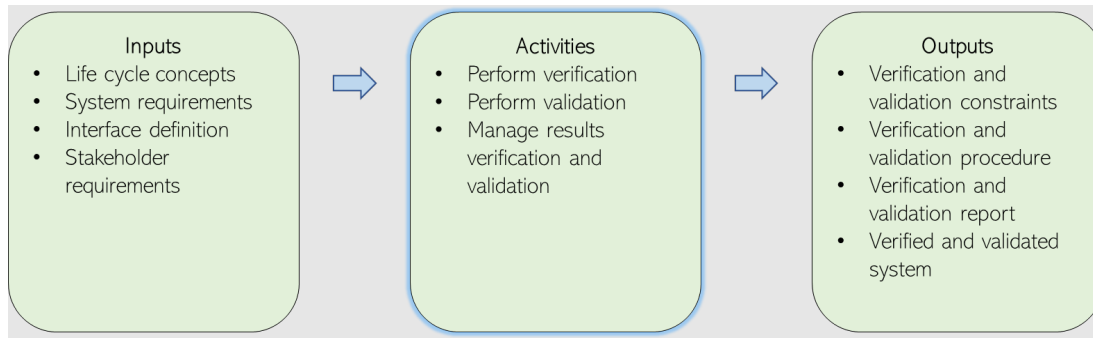


Figure 10. Verification and Validation Process Input Process Output (IPO) Diagram. Adapted from Walden et al. (2015).

The reviews in Table 4 were performed to assess the adequacy of the system design, and to demonstrate and test the ability to meet the requirements within cost and schedule.

Table 4. Reviews and Their Purposes

Review	Purpose
System Requirements Review	To ensure the system requirements are stable, consistent, and can be achieved within acceptable levels of risk using available technologies.
Interim Project Reviews	To monitor the progress of the project, including cost, schedule, and technical performance.
System Verification Review	To ensure the system requirements have been met and documented so that stakeholders can understand the capabilities and limitations of the product.

III. BACKGROUND AND LITERATURE REVIEW

This chapter presents a background and literature review from a broad base of reference materials including reports and journal articles from academia, industry, and government. Federal and DOD policies are also identified and summarized in this chapter.

A. BACKGROUND

There are various topics that need to be considered when creating a unified LBTS, including cybersecurity, connectivity, and communication. In this section, DOD and other federal cybersecurity policies are reviewed and actions that need to be completed prior to utilizing the system are identified. The security and communication baselines used in a test and development environment were also identified to determine how it correlates to the LBTS. The DOD has several networks used for different aspects of defense, from internets to intranets, and in support of varying levels of classification. DOD networks that can support One Navy Lab's unified capabilities are also identified and detailed in this section.

1. Joint Information Environment (JIE)

With the increasing global threats, it is imperative that DOD revolutionizes its digital environment to remain competitive in this dynamic environment. DOD CIO's approach in adapting to this changing environment is to "increase technological capabilities across the Department and strengthen overall adoption of enterprise systems to expand the competitive space in the digital arena" (DOD 2019, 3). To meet its objectives, the DOD CIO and other agencies have been implementing programs and projects anticipated to achieve DOD digital modernization strategies. The DOD CIO has also endorsed the JIE, a framework to "improve mission effectiveness, increase cybersecurity, improve interoperability, deliver capabilities faster, and realize IT efficiencies" (DOD 2019, 35). The JIE Framework is used to prevent cybersecurity attacks with its new joint cybersecurity capability, to facilitate networking for fixed and mobile users through its various networks, and to modernize DOD technologies through innovation (DOD 2019, 35). Table 5 shows the JIE capability objectives, their initiatives, and how they correlate to the DOD CIO objectives.

Table 5. Joint Information Environment (JIE) Objectives. Adapted from Department of Defense [DOD] (2019).

JIE Capability Objective	JIE Initiatives	DOD CIO Objectives
Modernize Network Infrastructure	Optical Transport Upgrades, Multi-Protocol Label Switching (MPLS) Routers Buildout, Asynchronous Transfer Mode (ATM) Switch and low speed Time Division Multiplexed (TDM) Circuit Elimination, Satellite Communications Gateway Consolidation and Modernization, Internet Protocol version 6 (IPv6) Implementation	- Modernize Warfighter Command, Control, Communications, and Computer (C4) Infrastructure and Systems - Modernize Defense Information Systems Network (DISN) Transport Infrastructure - Modernize and Optimize DOD Component Networks and Services
Enable Enterprise Network Operations	Establish global and regional operations centers, Establish the JIE Management Network, Converge IT Service Management (ITSM) solutions	- Modernize and Optimize DOD Component Networks and Services - Shift from Component-Centric to Enterprise-Wide Operations and Defense Model
Implement Regional Security	Joint Regional Security Stack (JRSS), Joint management System (JMS)	Modernize DISN Transport Infrastructure
Provide Mission Partner Environment (MPE)	Virtual Data Center, Applications and Services, MPE Transport, Mission Partner Gateways	Strengthen Collaboration, International Partnerships, and Allied Interoperability
Optimize Data Center Infrastructure	Data Center Optimization Initiative (DCOI) and Application Rationalization Initiative	Optimize DOD Data Centers
Implement Consistent Cybersecurity Protections	Enterprise Perimeter Protection Capabilities, Operate Securely in the Cloud, Endpoint Security, Data Center Security, Cyber Situational Awareness Analytic Capabilities (CSAAC)/ Big Data Platform (BDP), Identity, Credential, and Access Management (ICAM)	- Transform the DOD Cybersecurity Architecture to Increase Agility and Strengthen Resilience - Deliver a DOD Enterprise Cloud Environment to Leverage Commercial Innovation - Deploy an End-to-End ICAM Infrastructure
Establish End-User Enterprise Services	Enterprise Collaboration and Productivity Services (ECAPS)	- Optimize DOD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) - Optimize DOD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)
Provide Hybrid Cloud Computing Environments	Cloud Services	- Deliver a DOD Enterprise Cloud Environment to Leverage Commercial Innovation - Optimize DOD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1) - Optimize DOD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)

2. Cybersecurity Policies

To understand cybersecurity, one must first understand the concept of cyberspace. Ottis describes cyberspace as “a time-dependent set of interconnected information systems and the humans that interact with these systems” (Ottis et al. 2010, 267). Since the creation of the first computer network in 1969, cyber space has continued to expand and with it, an increase in “nefarious exploitation of this man-made domain” (Roesener et al. 2014). Given the integrated nature of defense systems, power grids, and the general internet of things (IoT), cyber-attacks can pose a serious threat to national security. This prompts the need for clearly defined policies to be implemented throughout the government. Cybersecurity is described as the “measures government institutions take to protect the public and the institutions themselves from threats” in cyberspace (Bay 2016, 4).

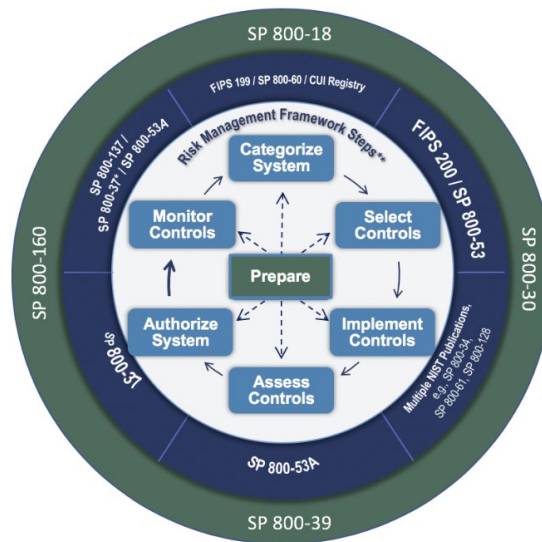
a. Federal Law

Federal Information Security Management Act (FISMA) is the governing law for cybersecurity. According to the act, the National Institute for Standards and Technology (NIST) is responsible for determining the appropriate security controls required for an information system based on its associated risk. For DOD agencies to comply with FISMA standards, an Authorization to Operate (ATO) must be developed. The ATO is a decision by a senior government official, the Authorizing Official (AO), that authorizes an agency to operate an information system on their behalf. The ATO implements an approved set of security measures and accepts the assessed potential risks to the operations, assets, and individuals within an organization, other organizations, and the nation (National Institute of Standards and Technology [NIST] n.d.)

b. DOD Cybersecurity Policies

The DOD cybersecurity program is described in DOD Instruction (DODI) (2014) 8500.01. The goal of the instruction is to ensure that DOD systems are used in a way that ensures confidence in the confidentiality, integrity, and availability of the system and digital information (DODI 2014). The management of cybersecurity risks is a complex process that involves assessing, understanding, and managing the risks associated with the use of digital information and systems. It requires a comprehensive approach that includes

the implementation of technical, organizational, and administrative measures to protect against potential threats.



(1) Step 1: Categorize System

The categorization results are documented in the security, privacy, and supply chain risk management plans (DODI 2022). The AO will have the final say in determining the categorization of the system.

(2) Step 2: Select Security Controls

The next step is to select the security controls. Security controls are defined as “safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk” (Joint Task Force 2020). A continuous monitoring strategy as well as a system security plan (SSP) will need to be developed to assess the controls throughout the system’s life cycle. A lab connected to a network will have approximately 50% more controls than an enclaved lab. As the number of controls increases, the amount of time and resources needed to implement and monitor them also increases. This means increased costs for the organization.

(3) Step 3: Implement Controls

This step defines how the system meets the security controls (Open Control n.d.). Any changes to the planned implementation of security controls will need to be reflected in the SSP.

(4) Step 4: Assess Security Controls

The security controls will then be tested in step 4. The assessment will include tests for the controls in the SSP and penetration test (AdHoc n.d.). Any actions to correct discrepancies found in the assessment will have to be completed and subsequent remediation actions will need to be documented in the SSP.

(5) Step 5: Authorization

The AO will then decide whether to grant or deny the ATO based on the risk posed by the system. This risk-based decision will be based on the authorization package, which includes the SSP, privacy plan, security control plan, privacy control assessment, and any other relevant documentation (AdHoc n.d.).

(6) Step 6: Monitoring

As part of the continuous monitoring strategy, the system and environment will continue to be monitored and tested. The results of the monitoring are analyzed, and any issues are addressed accordingly and documented in the authorization package. Any changes in risk acceptance will be communicated to the AO and authorizations will continue based on results of the monitoring (DODI 2022). Figure 12 shows the cybersecurity RMF process with respect to the system acquisition life cycle.

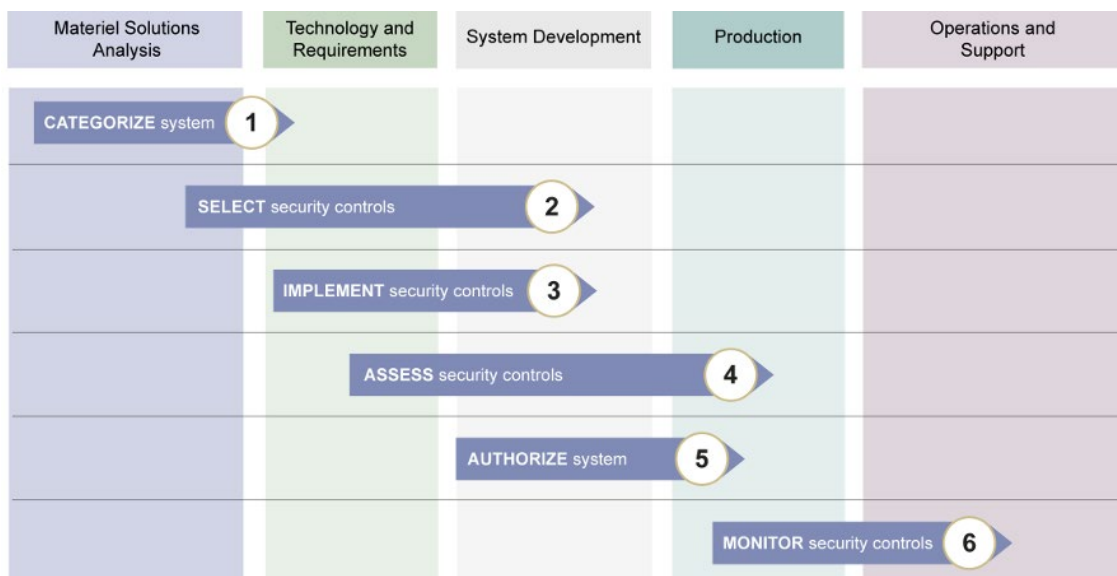


Figure 12. Department of Defense Risk Management Framework (RMF) in Acquisition Cycle. Source: Russell (2021).

3. Zones Environments

A zone breakdown is used to form the security baselines used in a test and development environment when one needs to isolate security environments (Defense Information System Agency [DISA] 2022). Architecture, remote access, development, and testing and evaluation are the components emphasized by the zones, and the architecture, as shown in Figure 13, “describes policy and placement of network infrastructure to ensure security of the agile environments” (DISA 2022, 5). There are four types of Zones, also known as enclaves: Zone A, Zone B, Zone C, and Zone D. An enclave is defined as “a

collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security, with its primary connection to the Defense Information Systems Network” (DISA 2022, 4). One example of an enclave is a local area network (LAN). Before connecting to outside networks, “all zones must be documented and the infrastructure certified with an Interim Approval to Operate (IATO)” (DISA 2022, 5).

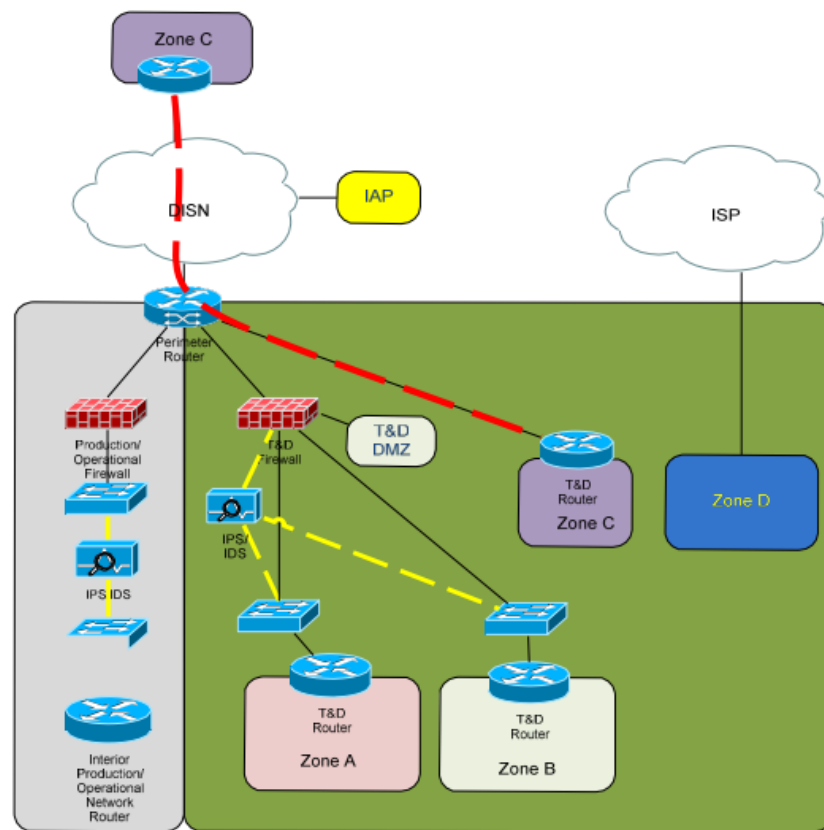


Figure 13. Example of Zones Architecture: Source: Defense Information System Agency [DISA] (2022).

Zone A environment is used during the final step of testing since it allows “connectivity to the live operational network for final testing prior to the product or application deployment into the operational network” (DISA 2022, 7). It mimics the operational network, and it has direct connectivity to external DOD networks (DISA 2022).

According to DISA, Zone A's framework must meet the DOD and federal requirements, and a connectivity authorization, an IATO at a minimum, must be obtained prior to connecting the system; additionally, virtual private network (VPN) must be utilized when remote access is needed (DISA 2022).

Zone B environment is similar to Zone A "from a network connectivity perspective but with much stricter control mechanisms" (DISA 2022). It is usually used "for moving sanitized data ... along with development of applications destined for a live and operational DOD network" (DISA 2022, 8). It has indirect connectivity to external DOD network and a firewall is used to separate it from the other zones (DISA 2022). An encrypted connection is required to access Zone B environment and VPN must be terminated before accessing the zone (DISA 2022). As is required for Zone A, Zone B's framework must meet the DOD and federal requirements and a connectivity authorization must be obtained prior to connecting the system.

Zone C environments are used when an organization needs to connect with other organizations to form "a fully closed multi-environment network for product testing and evaluation" (DISA 2022, 9). Proper documentation, such as memorandums of understanding and memorandums of agreement, must be used to facilitate communication and collaboration between the organizations involved (DISA 2022). Zone C environments are isolated from external DOD networks, so data are transmitted by tunneling such as tactical local area network encryptor (TACLANE) (DISA 2022). Therefore, data being transmitted must be encrypted to the highest required standard. A connectivity authorization must be obtained prior to connecting the system and all the DOD and federal requirements must be met.

Zone D environment is used when outside traffic is undesired. It is fully closed and isolated with no connectivity to any DOD network (DISA 2022). A connectivity authorization must be obtained prior to connecting the system and all the DOD and federal requirements must be met.

4. DOD Networks

There are multiple DOD networks currently available for R&D. It is essential to identify and analyze each network to determine if it meets the needs of the One Navy Lab. The following DOD networks are reviewed to evaluate the best options for the One Navy Lab.

a. Joint Mission Environment Test Capability Multiple Independent Levels of Security Network (JMN)

The Joint Mission Environment Test Capability (JMETC) was established in 2006 under the Test Resource Management Center (TRMC) to provide distributed test capabilities and simulations. The capability offers a “robust distributed infrastructure [such as] network, enterprise resources, integration software, tools, reuse repository...technical expertise” to allow for testing and evaluation within the Joint System of Systems and Cyber environment (Test Resource Management Center [TRMC] 2019, 2).

JMETC uses a hybrid network architecture consisting of the JMETC Secret Network (JSN) and the JMETC Multiple Independent Levels of Security (MILS) Network (JMN) (TRMC 2019, 14). For all classifications and cyber testing, the JMN is the enterprise network solution, aiming to provide secure distributed testbeds within multiple domains. To achieve this, the MILS architecture is used, which allows data streams to be segregated. One capability that sets JMN apart is the ability to emulate a ship network with exception to the latency.

b. Joint Mission Environment Test Capability Secret Network (JSN)

The JSN has been functional and growing since 2007. Using Secret Defense Research and Engineering Network (SDREN) as a backbone, JSN offers solutions for secret test and evaluation (T&E) efforts. It uses persistent connectivity as opposed to the event specific links JMN offers. The persistent connection enables users to execute testing without network coordination. Additionally, JSN offers end to end network monitoring, troubleshooting, and optimization (TRMC 2019, 16). Currently there are 49 JSN locations with access to 82 labs/facilities (TRMC 2019, 16).

c. *Joint Information Operations Range (JIOR)*

The Joint Information Operations Range (JIOR) was created to integrate test ranges for the DOD. The network uses a “type-1 bulk encrypted tunnel [which is a] VPN that carries several type-3 encrypted VLANs [virtual local area networks]” between sites (Joint Staff Public Affairs 2015). JIOR can operate in both persistent environments as well as tactical event environments. Like JMN, JIOR can also emulate a ship network.

d. *Defense Research and Engineering Network (DREN)*

“The Department of Defense established the High Performance Computing Modernization Program (HPCMP) to provide DOD scientists, engineers, and acquisition professionals with the computational resources needed to develop robust solutions to technical challenges” (High Performance Computing Modernization Program [HPCMP] n.d.). The HPCMP’s Defense Research and Engineering Network (DREN) is an “information-assured wide-area network that minimizes the impact of distance on time-to-solution” by providing flexible, low-latency, high-throughput communications (HPCMP 2016). Such a network supports the research, development, test and evaluation (RDT&E) and acquisition engineering communities. The third generation of DREN, “DREN III, offers bandwidth capacities starting at 50 megabits per second (Mbps) and [rising] to 100 gigabits per second (Gbps)” (HPCMP 2016). DREN connects to the DOD RDT&E and acquisition communities and acts as a backbone for the DOD test and evaluation community. In fiscal year (FY) 2016, DREN had “163 active sites ... located across the continental United States, [as well as] six peering points, two internet transit points, and three DOD private peering points for Non-Secure Internet Protocol Router Network (NIPRNet) peering” (HPCMP 2016). There are currently “38 other national and international networks including research and education networks” peering with DREN (HPCMP 2016).

e. *Secret Defense Research and Engineering Network (SDREN)*

SDREN is DREN’s secret level counterpart. The SDREN network overlay is implemented on the DREN backbone to support classified communications. SDREN is

often used to conduct classified test events. SDREN had 71 active sites in fiscal year 2016 (Rhoades 2008).

5. Testing Communication and Computer Networks: An Overview

The use of computers and communications in organizations today has become increasingly important. Networks are integral to distributing information and resources to employees, users, and customers within organizations across various sectors. These sectors include the scientific, manufacturing, social, and financial sectors. Networks must support various applications and services to guarantee seamless voice, video, and data delivery. Several factors contribute to the increased complexity of multi-vendor, multi-protocol networks, including adding new nodes, relocation of users, redistributing network resources, and interconnection of more subnets.

It is crucial to ensure the quality of service in this context, in which network testing and performance measurements are performed. The presence of some applications with performance-critical requirements necessitates the measurement of quality of service (QoS). In response to these evolving needs, the research community in instrumentation and measurement (I&M) faces significant challenges (Angrisani and Narduzzi 2008).

An overview of the measurement context, commonly used instruments, procedures, and critical issues associated with network testing is provided in the article. Measurement testing includes physical layer testing for devices and interfaces, which involves measuring their electrical or optical properties. As part of the network communication process, the higher-level protocol layers are tested, mainly levels 2 and 7 of the Open Systems Interconnection (OSI) models. Another measurement context includes the use of protocol analyzers on the major functions, such as protocol decoding, protocol statistics, expert analysis, and traffic flow measurement. Analyze timing and synchronization to determine if the network is meeting the increasing link speed and accuracy needs of users.

B. LITERATURE REVIEW

The literature review was completed to understand the current stage of research on a unified LBTS and to identify any questions that require further research. The works

discussed here are chosen due to objectives being similar to what is required of the One Navy Lab: integrating labs, cybersecurity considerations for a DOD network, and communication and data sharing over networks.

1. Mission-Integrated Network Control

The Defense Advanced Research Projects Agency (DARPA) created a Mission-Integrated Network Control (MINC) program to guarantee that essential data are clearly communicated to the appropriate personnel in a timely manner (Schurgot 2021). The MINC approach is designed to mix legacy and future systems to create new capabilities of tactical networks (Schurgot 2021). The One Navy Lab project can use a similar approach by applying the MINC development and integration of their key capabilities, including the creation of an “always-on” network and using a cross-network and a mission-driven approach (Schurgot 2021).

2. Integrated Tactical Network

The U.S. Army currently has an Integrated Tactical Network (ITN) project, which is a critical component of the Army’s Unified Network Plan. The ITN is a combination of communications and networking system that provides communication capabilities to tactical units in a congested and contested environment, as shown in Figure 14. During the development of the ITN, after each event, changes were made to the software and configurations to improve the performance of the network. The One Navy Lab will use a similar strategy, as it is effective for designing a system-of-systems network.

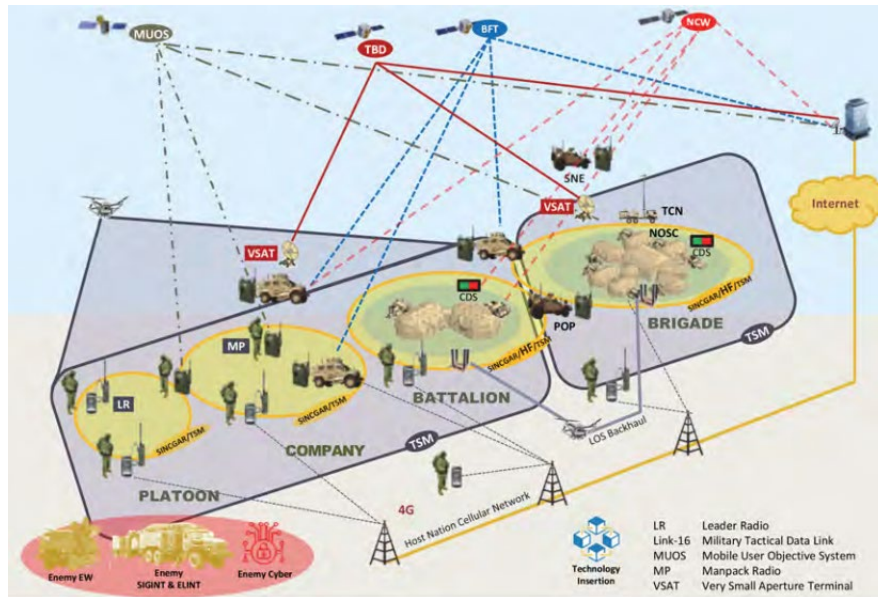


Figure 14. Integrated Tactical Network (ITN) Operational Viewpoint (OV)-1.
Source: Director, Operational Test & Evaluation [DOT&E] (2020).

3. Zero Trust Strategy and Roadmap

In November 2022, the DOD published its Zero Trust Strategy and Roadmap, which describes how it plans to reduce network attacks, enhance risk management, and improve data sharing (Lopez 2022). In addition to the basic cybersecurity defense tools, this new approach provides a framework for anticipating a breach and taking appropriate action based on that assumption (Lopez 2022). A similar approach can be used by the One Navy Lab to “prevent adversaries from attacking the...network and minimize damage” when an attack occurs (Lopez 2022). Assuming that the network has already been compromised, additional security measures will be implemented. As a result of this approach, an adversary could be identified and prevented from moving through the network.

4. Live Virtual Constructive

In an effort that seeks to eliminate onboard technical assists and provide Live Virtual Constructive (LVC) training, NSWC PHD connected the command’s network to the Navy Continuous Training Environment (NCTE). The NCTE is described as an environment that “consists of networks, simulations, simulation routing equipment, data

translation devices and live training range systems used together to create a realistic LVC training environment” (Ball 2021). In accordance with its name, LVC incorporates three aspects: live, virtual, and constructive. The term live refers to a real environment where users are operating a real system in a simulated environment, virtual refers to users operating simulated systems, and lastly constructive refers computer generated forces in a simulated environment. A combination of live, virtual, and constructive environments provides sailors with an ideal training environment. Information gathered from LVC and NCTE architecture will be used to support the capstone project.

5. Navy Center for Advanced Modeling and Simulation

The Navy Center for Advanced Modeling and Simulation (NCAMS) uses a joint network for “training and testing in support of fleet readiness, exercises and wargaming, as well as concept generation and experimentation” (Quick 2021). Information about the infrastructure and components of the NCAMS’s network will be leveraged to support this capstone project. The NCAMS’s network’s ability to send simulations to dispersed geographical locations aligns with the One Navy Lab’s goal of facilitating collaboration between engineers and technicians from different surface warfare centers. Additionally, NCAMS can be used to generate simulations in support of analysis of the proposed LBTS configurations in this report in order to evaluate the potential benefits and assess the potential risks associated with them. The use of NCAMS’s simulations would enable a more thorough analysis of the proposed One Navy Lab alternatives and aid decision-making of their implementation.

6. Remote Software Deployment

A technical report titled “Common Combat Systems Remote Software Deployment of Incremental Capability and Updates” was also reviewed by the team. It proposes a remote software deployment system for updating combat systems (Carter et al. 2020). As a result, the report demonstrates the feasibility of implementing remote deployment systems and outlines the capabilities gained. However, the report does not elaborate on each system’s interface requirements in detail. The team will provide an integration framework that will elaborate on each system’s interface requirements in detail and

describe the specific methods and techniques employed to ensure successful integration of new capabilities, updates, and system improvements.

7. Euronet Lab

The Euronet Lab: Euronet LAB, a cloud-based virtual lab environment lecture, discusses a proposal for developing a system that integrates various virtual lab platforms and components. To accomplish this, communication mechanisms must be established and interconnected. This paper addresses the challenge of connecting systems developed in different languages and cultures across geographically distant locations. Using the proposed plan, users can connect multiple virtual and remote labs over the internet. As a result, they can perform testing using components from different systems, regardless of their physical location (Cordeiro and Fonseca 2010). Gathering information from this proposal on methods of structuring an integrated network environment enables the team to create a framework to support the capstone project.

8. Implementing Engineering 2000

Engineering 2000 was a project in the Tomahawk community to create an architecture for sharing messages, documents, and other management tools for localized sharing. According to Page and Reese (1996), “One aspect of Engineering 2000 involves the development of a community-wide ‘network of networks.’ This computer network must give a geographically distributed set of government and contractor entities an improved ability to access and exchange mission-critical information.” This thesis has valuable information within it, such as the well-defined requirements and definitions of what is involved in their system that makes it easy to understand for all readers—for example, when Page and Reese (1996) define what the “network” and its “applications” are and what they are expected to do. The goal of the thesis was to design the framework and architecture for implementing Engineering 2000. The Engineering 2000 project has a very similar topic and end goal as the One Navy Lab’s; both are trying to integrate geographically distanced labs via a common network upon which information that opens new capabilities can be shared. One Navy Team can use the methodology and network determination that the Engineering 2000 report formulated.

C. SUMMARY

Reviewing prior work supported the research with developing a baseline of past and current efforts conducted to realize similar systems and their integration. The team identified areas in the prior works wherein improvements can be made to avoid similar problems in the One Navy Lab project. Additionally, the published networks and standards set up a baseline for the team from which to build the project up. Finally, the information gathered from these prior works were used as references to support the capstone project. The prior work reviewed helped to support the process to ensure the project meets the needs of the end user.

IV. STAKEHOLDERS NEEDS AND REQUIREMENTS ANALYSIS

A stakeholder is defined as “anyone who is materially affected by the outcomes of your project” (Bennett 2022). To satisfy their desire for a One Navy Lab, the stakeholder needs were required to be established to identify the guiding factors for a solution to the question: is One Navy Lab a more advantageous alternative to the current set-up? After identification of the stakeholders, One Navy Team was able to use stakeholder-provided documentation and references to capture primary interests and extract the needs for the One Navy Lab capstone project. The team followed the SE process to ensure needs and requirements align effectively with the scope of the One Navy Lab. The following sections detail the stakeholders, needs, and requirements analyses that were conducted.

A. STAKEHOLDER

One Navy Lab’s stakeholders were identified, as shown in Table 6. The stakeholders’ level of involvement and the respective primitive needs regarding the One Navy Lab were identified. The stakeholders’ primitive needs were used in the report to elicit One Navy Lab needs in a comprehensive manner.

Table 6. Stakeholders

Stakeholders	Prioritization	Level of Involvement	Primitive Need
NSWC PHD	Primary	Primary expert consultant for the One Navy Lab.	Interested in utilization of a lab validation framework to establish the One Navy Lab.
Vision Owners (Richard Watanabe, Craig Tenhoff, and Matthew Cole)	Primary	Primary expert consultant for the One Navy Lab.	Interested in utilization of a lab validation framework to establish the One Navy Lab.
Users (Engineers and technicians employed by NSWCs)	Secondary	Integrate, use, maintain, and modernize the lab.	Interested in the use of the One Navy Lab.

B. NEEDS ANALYSIS

Following the major stakeholders' identification, the team entered the needs analysis process. The following needs were identified:

- Enhance collaboration between geographically separated labs.
- Improve efficiency of software and hardware R&D.
- Conduct integrated combat systems testing prior to fielding.
- Increase PHD's capability as ISEA.
- Conduct real-time investigations for shipboard combat systems discrepancies.
- Technical documentation development and verification on shipboard representative equipment.
- Interoperability system training for technicians and engineering supporting naval combat systems.
- Reduce schedule delays by making full use of the resources available.
- Validate product performance prior to shipboard installation.
- Reduce travel costs related to shared lab usage.
- Reduce dependencies on original equipment manufacturer (OEM) labs.
- Validation framework for the integration of labs.

The needs “represent the views of...users, acquirers, customers and other stakeholders as they relate to the [system]” (Faisandier, n.d.). One Navy Lab seeks to satisfy the needs identified or relay why they cannot be accomplished.

C. USE CASES

The following use cases (UCs), visually represented in Figure 15, outline the operational concept of the One Navy Lab:

- [UC-1] Fleet Support: Fleet Support personnel will be able to replicate the system environment to quickly diagnose and resolve discrepancies.
- [UC-2] Testing: Testers will be able to mimic shipboard environments with an integrated lab environment. This helps identify issues early and avoid costly delays.
- [UC-3] Developing technical documentation: Technical documentation developers will be able to take advantage of the shared resources brought by the integrated labs. This in turn produces more accurate documentation and limits traveling delays due to limited system resources.
- [UC-4] Hardware/Software Development: By using integrated labs, hardware and software developers can ensure hardware and software components are thoroughly tested in a shipboard representative integrated environment before implementing them onboard ships.
- [UC-5] Training: Integrating labs will give trainers the ability to replicate battle scenarios in a CMS environment to train and maintain sailor battle competency.

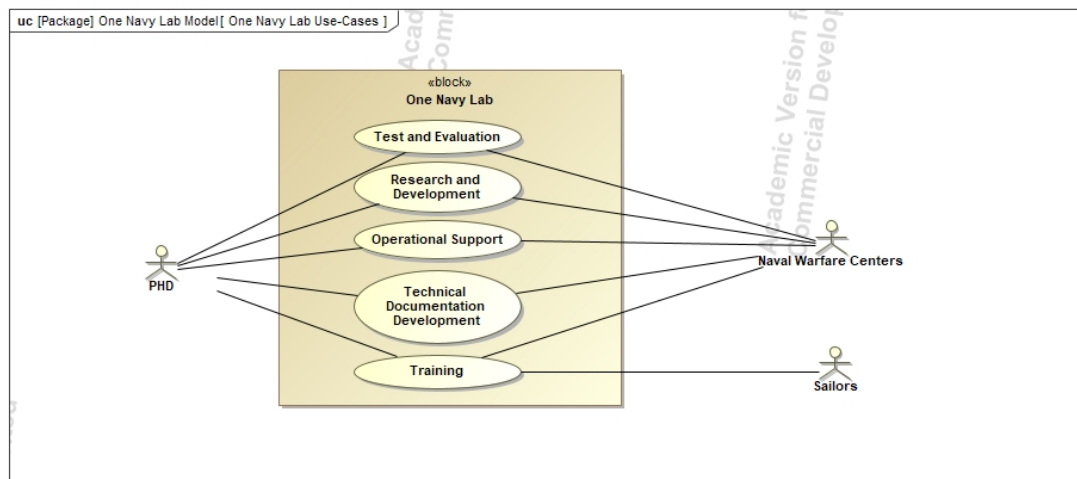


Figure 15. One Navy Lab Use Cases

D. REQUIREMENT ANALYSIS

A requirements analysis was performed by gathering the stakeholders' needs and transforming them into system requirements to meet the operational needs of the One Navy Lab. The inputs to the requirements analysis consisted of the stakeholder objectives, and the current and future capabilities obtained from the stakeholder-provided documentation and the literature reviews. The requirement analysis generated a list of high-level functional requirements describing the One Navy Lab's primary functions as shown in Table 7.

Table 7. High-Level Requirements

ID	Requirements
1	The system shall comply with DOD security standards.
2	The system shall be reliable.
3	The system shall be available.
4	The system shall support testing activities.
5	The system shall support training activities.
6	The system infrastructure shall be flexible to support system modifications.
7	The system shall be able to include multiple naval combat shipboard systems.
8	The system shall integrate with other naval facilities.

Upon completion of the requirement analysis, a functional analysis was performed to transform the high-level functions into lower-level functions. Table 8 displays the functional requirements.

Table 8. Low-Level Requirements

ID	Requirements
1.1	The system must align with the NIST guidelines.
1.2	The system shall comply with DOD Instruction (DODI) (2014) 8500.01.
1.3	The system shall align with DODI (2016) 5200.01
1.4	The system shall comply with FISMA.
2.1	The system shall support combat systems elements interface requirements.
2.2	The system shall ensure integrity of data.
3.1	The system shall have a down time of no more than 128 hours per week.
3.2	The system shall have an inherent availability of 90%.

ID	Requirements
4.1	The system shall support operational testing.
4.1.1	The system shall support intra-element system testing.
4.1.2	The system shall connect a CMS to a weapon system.
4.1.3	The system shall connect a CMS to a sensor system.
4.2	The system shall support a system performance test.
4.2.1	The system shall support a kill chain test.
4.2.2	The system shall support endurance test.
4.2.3	The system shall support vulnerability testing.
5.1	The system shall support system operations training.
5.2	The system shall support system maintenance training.
6.1	The system shall have a flexible workspace to allow for addition of new elements.
6.2	The system shall have a workspace with flexible cable accommodations for addition of new elements.
7.1	The system shall include a weapon system.
7.2	The system shall include a radar system.
7.3	The system shall include a combat management system.
8.1	The system shall allow for collaboration of projects.
8.2	The system shall allow resource sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COURSES OF ACTIONS

Based on the stakeholders' needs, use cases, and derived requirements detailed in Chapter IV, the team proposes five COAs for the decision makers. The first COA is to maintain the current operations and the remaining four are varied set-ups. The five COAs are proposed as options that fulfill the stakeholders' desired needs. The four new COAs support having an integrated, shipboard representative environment for engineers and technicians to complete their work. The following subsections detail the architectures of the different COAs.

A. COA 0: ON-SHIP INTEGRATION

COA 0 is to keep the current working set-up and maintain having the ship as the first time any integration takes place. Additionally, engineers and technicians will continue traveling to other LBTSS, as seen in Figure 16, for their taskings if their own NSWC's LBTSS cannot support. As described in the problem definition in Chapter I, shipboard testing is the first opportunity for interoperability testing, and this COA retains that standard. Figure 17 details the elemental systems on a ship that define a fully integrated system for this report. This COA, as described previously, requires users to travel to LBTSS and ships if necessary and as a result they are dependent on the ships and labs' schedules on when they are available.

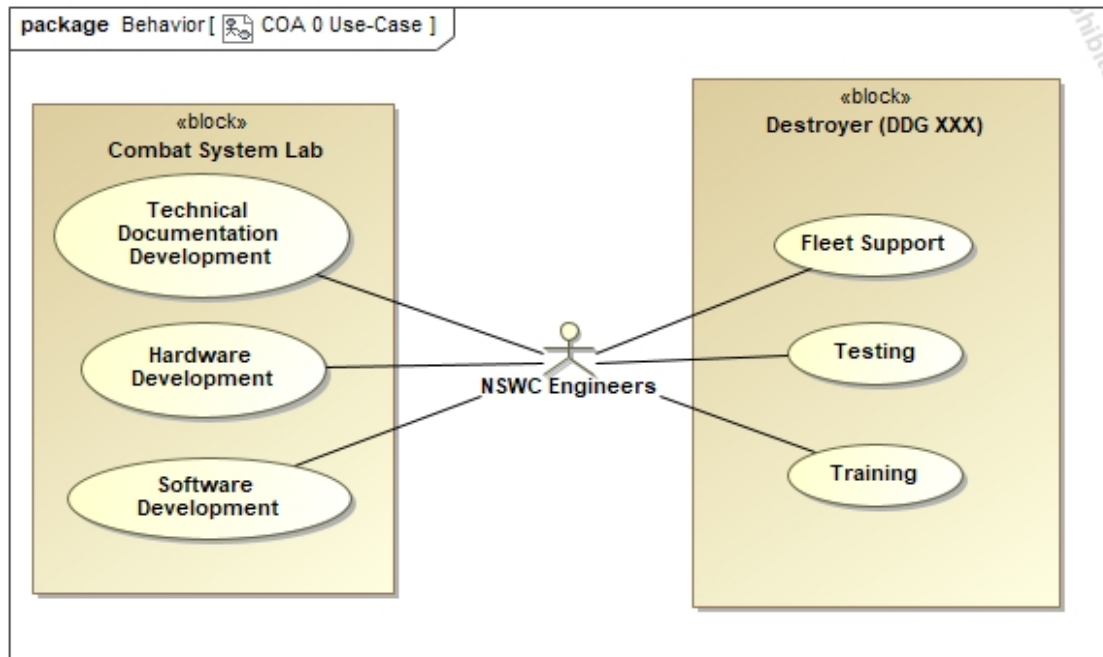


Figure 16. Course of Action (COA) 0 Work on Current Land-Based Test Sites and Ships

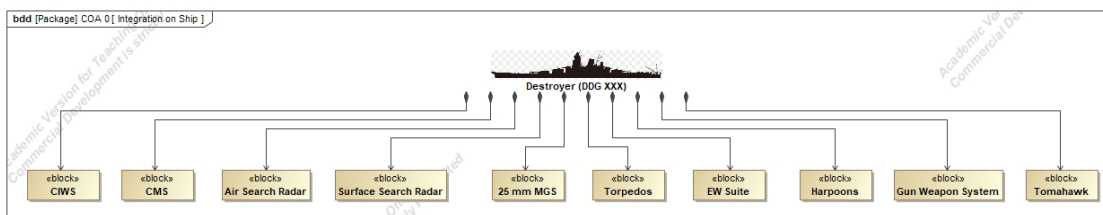


Figure 17. Course of Action (COA) 0 Architecture

B. COA 1: ONE INTEGRATED COMBAT SYSTEMS LAB

COA 1's One Navy Lab concept will be one fully integrated combat systems lab that will be shared by the different NSWCs. The lab will be located at one location in the U.S. and the various users will be required to travel to the lab. Figure 18 shows the architecture for one fully integrated combat systems lab with the elemental systems previously defined in COA 0. This COA will require development of a laboratory infrastructure at a geographical location selected by decision makes, and travel by the users from various NSWCs. The lab will be designed with extra space and modularity such that additional systems can be incorporated or replaced over the lab's lifetime, as required.

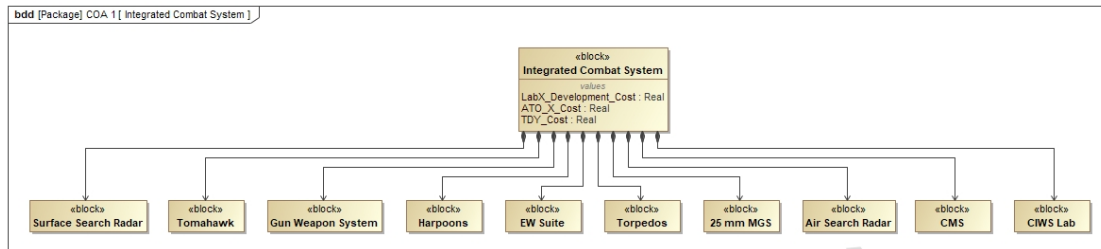


Figure 18. Course of Action (COA) 1 Architecture

C. COA 2: INTEGRATED COMBAT SYSTEMS LABS IN EVERY LOCATION

COA 2 is like COA 1, but the labs are duplicated in various locations chosen by the decision makers. As seen in Figure 19, this COA shows the integrated combat systems defined in COA 1 replicated at different NSWCs. This COA also requires development of, in this case multiple, laboratory infrastructures to house the integrated combat systems, with the same extra space and modularity to accommodate for the future changes. As each lab is at each respective NSWC location, travel costs will be avoided with this COA.

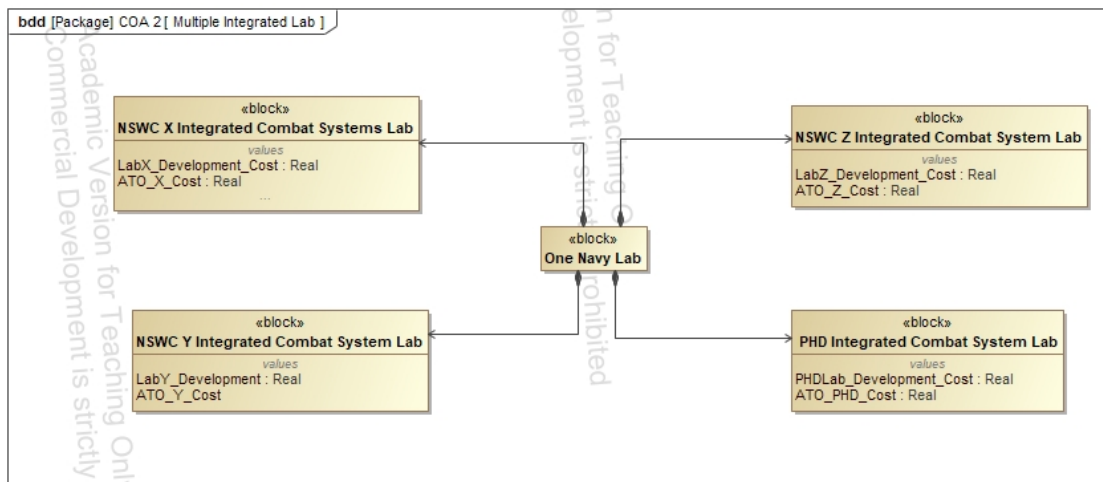


Figure 19. Course of Action (COA) 2 Architecture

D. COA 3: INTEGRATION VIA NETWORK

COA 3 is designed such that each separate NSWC will maintain the labs that they currently have, but the labs will be connected to a naval network so that all the labs on the

network can be accessed by all the participating NSWCs. All interfaces will be connected through a naval network, as shown in Figure 20. This naval network is dubbed by the team as the Navy One Lab Integrated Network (NOLIN). This interpretation of the One Navy Lab enables one NSWC command to access elemental systems of another NSWC command. COA 3 can build the team defined integrated combat systems without additional procurement costs, but it will require network operational and maintenance costs. Additionally, conversion of Zone D labs—isolated elemental labs—into Zone B labs—network connected elemental labs with firewalls and encryptions—will result in additional cybersecurity requirements that must be considered. As a result, the interface requirements between each system will also be impacted, as data traffic that was previously routed through a Zone D isolated LAN, is now required to travel via a wide area network (WAN).

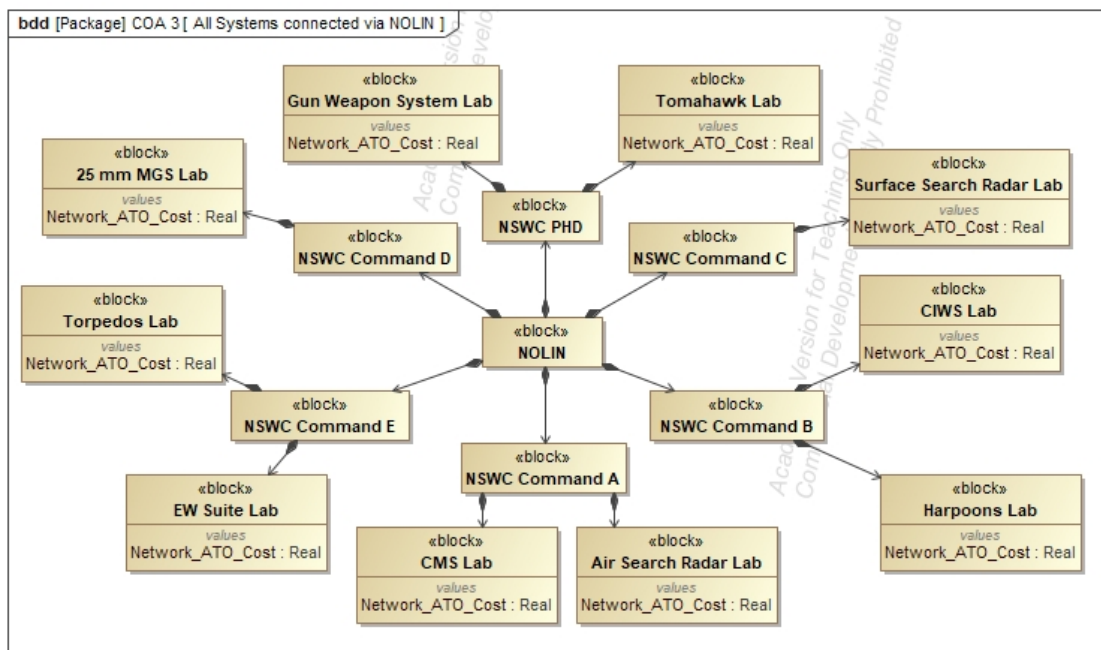


Figure 20. Course of Action (COA) 3 Architecture

1. Network Components

To implement COA 3, it must be understood what the implications are of the components of a network. The network has various quantifiable and verifiable

characteristics that influence the type of network that is necessary and can be selected. Additionally, the available naval networks must be analyzed and assessed for compatibility for the type of network the One Navy Lab requires. The following sections will detail the network characteristics and the various networks available.

a. Bandwidth

Network bandwidth is the “capacity for [the] speed...[and] speed refers to the rate at which data can be transmitted,” thus a bandwidth of 300 Mbps means that 300 megabits of data can be transferred each second (Froehlich 2021). It can be calculated by the amount of data per time. Real-world factors, such as channel physical characteristics, protocol used, network congestion, and environmental factors, affect bandwidth. The maximum bandwidth depends on the medium for transmission, equipment, and configuration of the network.

Depending on the function of a system, the bandwidth requirement will vary. It is expected that bandwidth requirements for voice transfer will range from 6 kilobits per second (Kbps) to 128 Kbps, while bandwidth requirements for video streaming will range from 50 Kbps to 6 Mbps, compared to real-time radar data, which is in the order of tens of Mbps to hundreds of Mbps (Banka et al. 2005). The bandwidth threshold will have multiplicity with respect to the amount of application being executed simultaneously. For example, if one video stream requires 6 Mbps, then 3 video streams will require 18 Mbps of available bandwidth. When utilizing this framework, Program Acquisition Research Managers (PARMs) should utilize actual system specifications to ensure the network can support the One Navy Lab requirements.

b. Latency

In computing, latency is the “time it takes for a packet of data to travel from source to a destination,” that is, the length of time from when user requested data to when they received the data (Mozilla Developer Network Web Docs 2023). Latency is the combination of transmission delays, propagation delays, queuing delays, and processing delays (Network Playroom 2017). In this case, the system’s performance can be adversely affected by the latency of the network.

Depending on the use case, the required latency will vary. The One Navy Lab use cases were categorized into two classes of computer applications: soft real-time applications and hard real-time applications, presented in Table 9 where the X's represent the use case's soft versus hard real-time applicability. Different applications have different requirements for how fast data is required to be transmitted with respect to the system's external environment. The team defines soft real-time application latency as having a latency up to 150 milliseconds (ms), this allows some leniency in the time allowed for the system to send over the data packet from NSWC A to NSWC B via NOLIN. Applications requiring soft real-time latency include remote desktop, voice over internet protocol (IP), and video over IP, among others. In contrast, military target-tracking applications have much stricter hard real-time latency requirements. A CMS needs to manage target tracks by receiving data from sensors and presenting it to the user in an organized manner that allows for weapon system engagements. This data includes information such as target position, speed, direction, and type. If the latency of the data is too high, the combat management system may drop targets due to the inaccuracy of the tracked targets. Due to the classified nature of these systems, latency interface requirements are not publicly available, but this report will assume a hard real-time application latency requirement of 1 ms. This value was obtained by taking Real-Time Innovations Inc. (2007) statement of a real-time weapon controller being sub-millisecond and rounding it up. When utilizing this framework, PARM should use values as stated in the capability development document (CDD) of the CMS.

Table 9. Real-Time Applications Latency

Use-Cases	Description	Hard Real-Time Applications	Soft Real-Time Applications
UC-1	Fleet Support	X	X
UC-2	Testing		
UC-2.1	Independent Verification and Validation		X
UC-2.2	System Integration Test		X
UC-2.3	Operational Kill-Chain test	X	
UC-3	Technical Documentation		
UC-3.1	Maintenance Requirement Cards	X	X
UC-3.2	Software Installation Procedures		X
UC-3.3	Standard Operating Procedures	X	X
UC-3.4	Technical Manuals	X	X
UC-4	Development		
UC- 4.1	Hardware Development	X	X
UC- 4.2	Software Development	X	X
UC-5	Training		
UC-5.1	Interoperability Training	X	
UC-5.2	Emulator Training	X	X

c. Jitters

NOLIN must integrate and support a wide variety of applications and services such as real-time voice, data, and video streaming. In real-time and interactive services, jitters—the measurement of packet transfer delay variation—remains an important quality of service parameter (Dbira, Girard, and Sansò 2016, 223). The operator should estimate and control the delay variation to prevent “buffer overflows, which cause packet losses, and buffer underflows,” which result in long delays between packets being received (Dahmouni, Girard, and Sansò 2011, 81–82). It is important for PARM to ensure the network can support low enough jitters so as to support the One Navy Lab’s objectives.

Real-time video streams should not have jitters exceeding 30 ms (Umenne and Odhiambo 2013). One Navy Team assumes that the same requirements apply for NOLIN. When PARM is utilizing this network, they should confirm the jitters are low enough to operate real-time services, such as radar data transmission or video streaming.

d. Security

Information exchange security is defined as the ability to secure dynamic information flow within and across domains. The security of information exchange is achieved by isolating data types and operational uses through physical and virtual isolation (United States Department of Defense [U.S. DOD] 2023). The use case scenarios will drive the classification of the domain. For example, a network simulating a fire control loop would have to support secret data transfer driven by the classification of the radar data. To ensure security, the network must have the capability to encrypt data before it is sent and decrypt it after it is received. This will prevent any unauthorized access to the data and ensure that only authorized users are able to view it. The encryption must be strong enough to withstand any attempts to hack or decrypt the data. The encryption should also be updated regularly to ensure its effectiveness.

e. Availability

The availability of a product is a metric that measures the probability that the product will perform its task when needed (Rockwell Automation n.d.). Inherent availability only considers a product's operating and corrective maintenance times (Defense Acquisition University [DAU] n.d.c.). It is important to note that the inherent availability of a network is significantly affected by its design, infrastructure, redundancy, and maintenance practices. Redundant network components and data paths are often used to minimize downtime which allows for high availability probabilities. The team assumed that all DOD networks would have at least a 90% inherent availability due to the redundant nature of networks. When utilizing this framework, PARM should confirm the availability of the network.

2. Analysis of Naval Networks

The team investigated existing DOD networks to help decision makers evaluate the best options that can help address the One Navy Lab's operational needs. While multiple R&D networks exist, the team focused on the networks described in the background section to leverage existing infrastructures.

The network matrix shown in Table 10 shows each network compared to the capabilities that are essential for One Navy Lab operational use, where check marks indicate the capabilities exist for specific networks. The matrix can be used to identify the capabilities each network provides and to determine which network can be used by NOLIN to support the One Navy Lab the best.

Table 10. Network Matrix

	Network Capabilities					
	Bandwidth 1 Gbps	Network Emulation	Operate in a Secret Domain	Operate in an Unclassified Domain	Operate in a Top Secret Domain	Inherent Availability of 90% or Greater
JIOR	✓	✓	✓	✓	✓	✓
JMN	✓	✓	✓	✓	✓	✓
JSN	✓		✓			✓
DREN	✓			✓		✓
SDREN	✓		✓			✓

3. COA 3 Key Performance Parameters

The team identified the functional requirements that must be met by the One Navy Lab to meet its operational goals. From those requirements, KPPs were established for the NOLIN to supplement decision making information for COA 3. KPPs are defined as “the minimum attribute or characteristic considered most essential for an effective military capability” (Defense Acquisition University [DAU] n.d.a.). Any deviation from the KPPs can have major impacts on the COA 3 system performance. COA 3's NOLIN must meet the KPPs listed in Table 11 in order for the One Navy Lab to meet its operational requirements.

Table 11. Network Key Performance Parameters

ID	KPP
2.1.1	The system connects separate labs via a network.
1.2.1	The system can connect at least 2 labs.
2.1.1	The system bandwidth for voice transfer must support 128 Kbps.
2.1.2	The system bandwidth for video streaming must support up to 6 megabits per second (Mbps).
2.1.3	The system bandwidth for streaming live radar data ranges from 10 Mbps to 1 Gbps.
2.1.4	The allowed latency for hard-time applications is less than 1 millisecond.
2.1.5	The allowed latency for soft real-time applications is less than 150 milliseconds.
2.1.6	The network data does not have jitters exceeding 30 milliseconds.

VI. MODELING AND SIMULATION

This chapter discusses the modeling and simulation of the One Navy Lab COA 3. The team developed system architecture diagrams to understand the interface relationships and physical limitations of the system. A simulation model was developed to evaluate the behavior of the system under specific circumstances. Once the architecture and simulation models were completed, further analysis was conducted on the interfaces between each lab. With the results of this approach, stakeholders will gain valuable information as to whether the system meets its KPPs. COA 3, in particular, was modeled and simulated because the infrastructure is new and undeveloped. The report develops a framework for the establishment of COA 3, and the modeling and simulation supports the framework analysis. COA 0 was not modeled as it is the current state of operations and thus is known to be functional. COAs 1 and 2 were not modeled and simulated because such naval laboratories have already been established currently. As mentioned in Chapter I, currently there are many combat systems labs distributed geographically across the United States and as a result the establishment of such labs is understood and proven to be possible.

A. ARCHITECTURE DESIGN

The architecture design process translates stakeholders' requirements into design solutions (Defense Acquisition University [DAU] n.d.b.). The team utilized the Department of Defense Architecture Framework (DODAF), which serves as the "principal guide for development of integrated architectures" (U.S. DOD 2023). The DODAF can be described in six steps, as shown in Figure 21. Steps 1–3 were covered in Chapters I-III of the report. In this chapter, the team covers collecting, organizing, correlating, and storing architecture, as well as conducting analyses and presenting results.

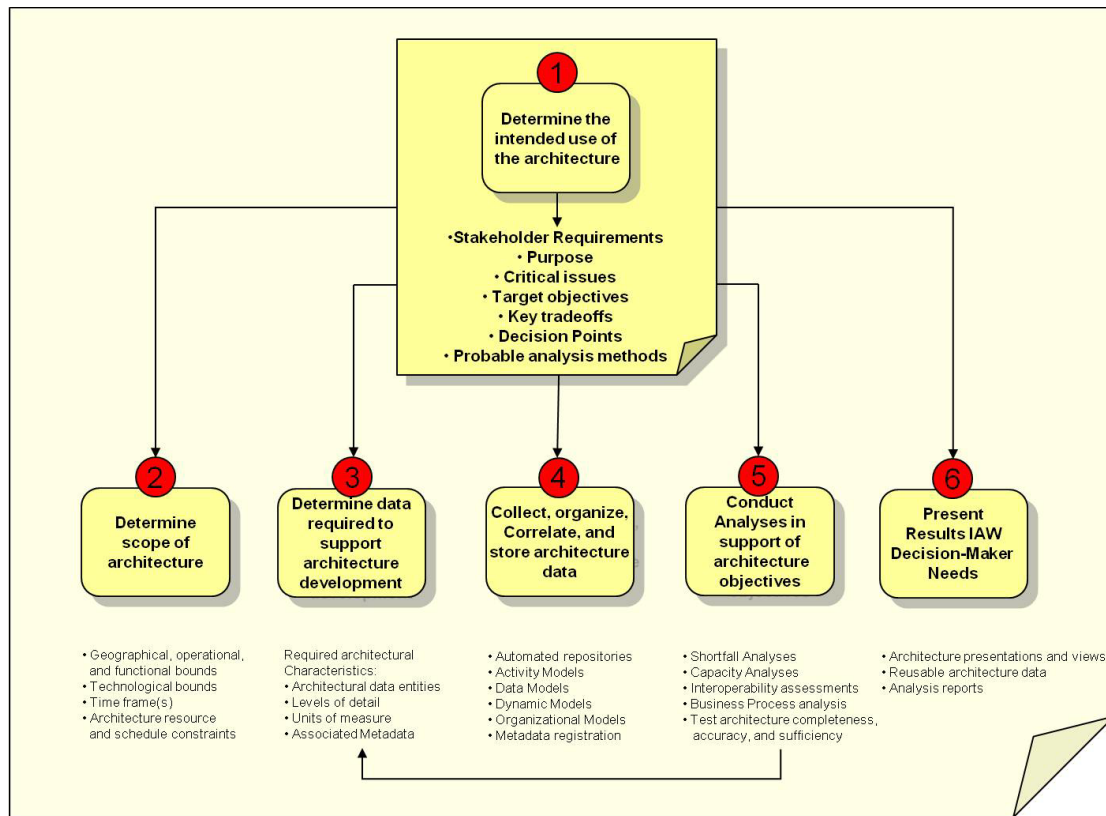


Figure 21. Department of Defense Architecture Framework (DODAF) Six-Step Process. Source: United States Department of Defense Chief Information Officer (n.d.).

1. Approach

Model-based systems engineering (MBSE) has improved the architecture design process by providing a systematic approach for developing, analyzing, and testing the system requirements. In this project, the MBSE Team utilizes Magic Systems of Systems Architect (MSOSA), a system modeling language (SysML) modeling tool, to build and understand the system architecture (Dassault Systemes 1981).

COA 1 and 2 are set up in the same configuration as COA 0, thus they are assumed to meet the interface requirement 2.1, listed in Table 8, as COA 0 does. The team must analyze the feasibility of COA 3 to confirm it can meet the KPPs listed in Chapter III. MSOSA and ExtendSim allow the team to visually represent the system architecture and

to identify key points of interaction and dependencies (Imagine That 1987). Based on the latency data obtained, the team is able to rank the feasibility probability of the COA.

To support COA 3, a DOD network will need to be implemented in each command that takes part in the One Navy Lab. The network, NOLIN, must operate in a highly virtualized environment. NOLIN must also have the capability to work in a secret level environment to accommodate classified data being exchanged within the integrated combat systems.

2. System Architectural Modeling

The team developed a system model to understand how each lab will connect to the network. Figure 22 illustrates the implementation of NOLIN in NSWCs and other R&D facilities. NOLIN system boundaries will end at the NOLIN nodes at each facility. Following this, the facilities' LAN will continue to transmit data to the appropriate systems. The NOLIN nodes act as firewalls, cybersecurity boundaries, and encryption devices. When assessing the feasibility of the objective, it is also necessary to consider the network infrastructure between the two labs. The overall system diagram allows stakeholders to visualize the full scope of the system, including the interface between each lab, the NOLIN nodes, and the network infrastructure. The diagram provides stakeholders with an understanding of the system architecture and helps to identify any potential physical limitations.

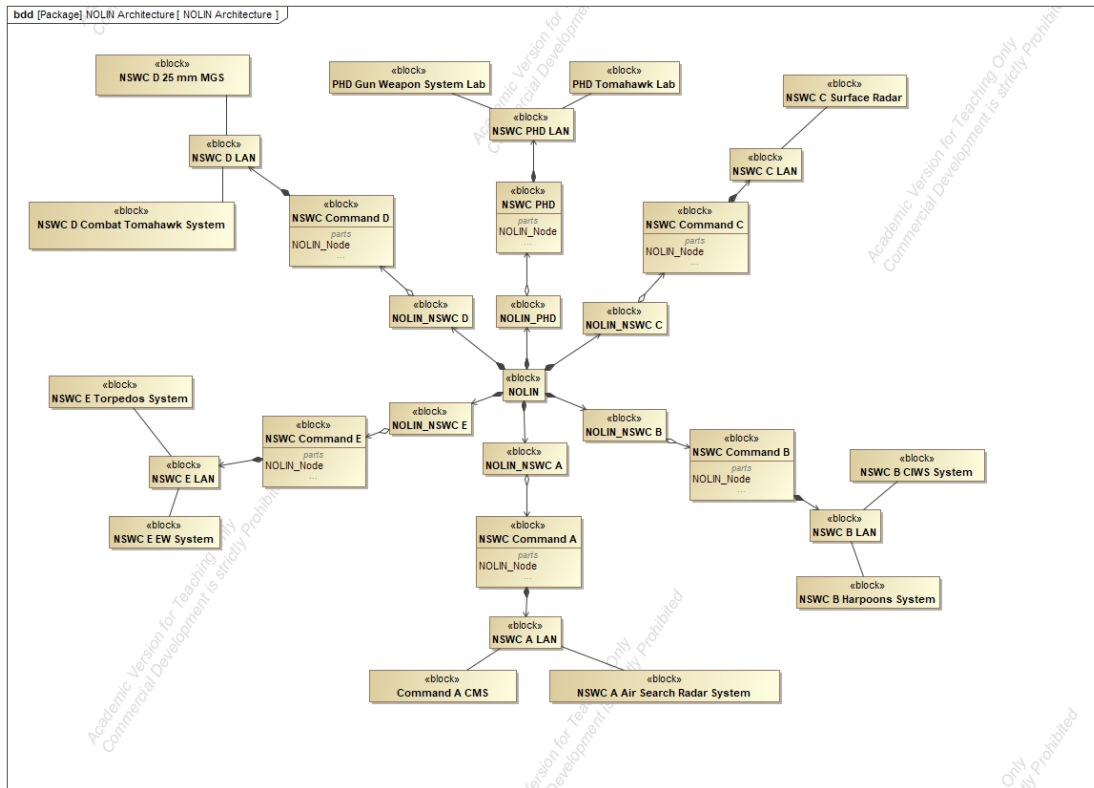


Figure 22. Navy One Lab Integrated Network (NOLIN) Architecture

B. NETWORK ANALYSIS

The One Navy Lab will use a network to exchange data from one laboratory to others in various geographical areas. The data being transferred over this network must have the same receiving situational environment as its delivering situational environment has. These sending and receiving environments are defined by a network protocol, which is an “established set of rules that determine how data is transmitted between different devices in the same network” (The Computing Technology Industry Association [CompTIA] n.d.). The two protocols being considered are the user datagram protocol (UDP) and transmission control protocol (TCP), which are the “most widely-used communication protocols in the Internet protocol suite” (Risk 2021). The main difference between UDP and TCP is that the former guarantees a more reliable transfer, and the latter guarantees a faster transfer (BasuMallick 2022). The networks’ latencies within the One Navy Lab are explored with a simulation. The following sections discuss the methodology

used for modeling network latency and provide an in-depth understanding of the factors contributing to the network delay within the One Navy Lab.

1. Simulation Methodology

The team chose to model and interpret the network data transfer through a discrete-event simulation. A discrete-event simulation was selected because it mimics best what happens with network data transfer, the “variables change instantaneously at separate points in time” (Law 2015, 6). This approach is grounded in the representation of distinct and quantifiable events and entities, mirroring the transmission of individual data packets between network nodes. These data processing events possess specific start and end times, aligning seamlessly with the principles of discrete modeling.

a. Protocol-Based Latency Analysis

Each proposed protocol has been researched to understand their impact on latency, which in turn affects the functional uses of the One Navy Lab. As mentioned previously, latency affects the One Navy Lab’s performance; a higher latency value means a slower data exchange between two labs. The two protocols affect this latency value due to the innate characteristics that are described in the following paragraphs.

(1) UDP versus TCP

One of the foundational aspects of the model is the choice of protocol. The UDP is a high-performance protocol; it “permits packets to be dropped instead of processing delayed packets...[and] there is no error checking...[thus] saving bandwidth” (Geeksforgeeks 2023). UDP is considered a “send-and-forget” method, which results in a unidirectional data transfer. The data packets get sent from the originating system through the UDP network, and the UDP protocol drops unsuccessful packets without attempting to resend the data packet. Then, it immediately moves onto the next data packet to send to the receiving system. Due to this, UDP is less reliable than TCP for complete data transfer but is a faster protocol, which results in a lower latency value. TCP, on the other hand, is a process that is a slower protocol due to it ensuring “the successful delivery of data and messages” (Fortinet n.d.). Thus, its iterative process of ensuring the integrity of the data

packet and its delivery means that the latency is higher, i.e., TCP is first in first out, so the packets need to wait in line until the one ahead of them has been delivered. Additionally, TCP requires every data packet received to be acknowledged due to it being an acknowledgement-based protocol; this adds additional time to each data packet transfer and as a result increasing the latency even more (Kumar, Manjunath, and Kuri 2008).

(2) MTU

The maximum transmission unit (MTU) represents the maximum size of a data packet transmitted over a network without fragmentation (Information Sciences Institute [ISI] 1981, 26). By assuming a packet size matches the MTU, the model ensures compatibility with a broad range of network configurations, for both modern and legacy equipment (Hornig 1984, 1). By adopting this assumption, it is possible to analyze network performance under a wide range of configurations. If the network cannot support MTU, then it can be concluded that any data packet sizes below that will have additional acknowledgement latency.

(3) Round-Trip Time

Within the simulation model, the team derives the round-trip time (RTT). This pivotal metric quantifies the duration of a packet's traverse from origin to destination (Acharya and Saltz n.d.). RTT is a fundamental yardstick for assessing network performance, and its meticulous analysis facilitates network design and optimization strategies. For scenarios involving the UDP protocol, which typically operates in a fire-and-forget manner, it is assumed that the network delay is the cumulative sum of five delay factors. Equation 1 sums the five network delay factors to provide each pack an attribute base delay. Each of these delay factors, discussed in the Network Delay Factors section, plays a distinct role in shaping the total RTT.

$$RTT = \sum \text{Network Delays Factors} \quad (1)$$

In stark contrast, when considering the TCP protocol, the delay increases two-fold due to a distinctive characteristic: the mandatory transmission of an acknowledgment message back to the sender upon successfully receiving a data packet. Equation 2, although

similar to the UDP equation, adds the acknowledgement—ACK—packet sent back to source when using TCP. This acknowledgment is a 46 bytes packet that travels back to the packet originator. This acknowledgment mechanism introduces additional latency, making TCP-based communication distinct from UDP’s swift and minimal latency, with the added benefit of increased packet success delivery rate. Recognizing this divergence in delay behavior is critical for devising strategies that accommodate other network protocols. This is also critical for optimizing network performance accordingly.

$$RTT = \sum \text{Network Delay Factors} + \sum \text{ACK Packet Network Delay Factors} \quad (2)$$

a. Network Delay Factors

Equation 3 denotes that for the following calculation, the sum of the network delay factors is also represented by total network delay (D). Equation 4 calculates the total network delay the model considers by summing the five critical factors: processing delay, serialization delay, router delay, transmission delay, and propagation delay (Ramaswamy et al. 2004). Processing delay measures the time between receipt of a request and response dispatch. Serialization delay accounts for the duration between transmitting a response and its reception by the intended recipient. Router queue delay represents the time lag from sending a request to its processing by a network router. Transmission delay quantifies the interval between sending a request and its arrival at the receiver. Propagation delay denotes the additional time signals to travel between network nodes. These delay factors collectively determine the speed and efficiency of data transmission between nodes, emphasizing the necessity of considering them all to optimize network.

$$D_{\text{Total Network}} = \sum \text{Network Delay Factors} \quad (3)$$

$$D_{\text{Total Network}} = D_{\text{Processing}} + D_{\text{Serialization}} + D_{\text{Router Queue}} + D_{\text{Transmission}} + D_{\text{Propagation}} \quad (4)$$

(1) Processing Delay

Within this model, processing delay assessment considers the impact of encryption and firewall processes. The duration of encryption delay varies based on the processing

speed of the central processing unit (CPU) and the precise specifications of the firewall equipment in use.

Equation 5 applies the concept, explained in K. Akdemir’s (2010) white paper “Breakthrough AES Performance with Intel AES New Instructions,” to calculate the encryption delay utilizing the AES-256 encryption protocol. An Advanced Encryption Standard (AES) is a symmetric encryption algorithm that uses—in this case a 256-bit—key to encrypt plain text or data (Zenarmor 2023). Widely use in the U.S. military, since it is practically unbreakable by brute force based on current computing power, it is considered the most secure encryption standard available. As a baseline, it is assumed a mid-tier CPU operating at 2.5 gigahertz (GHz) may exhibit a random deviation of approximately 10%.

$$D_{Encryption} = \frac{1.3 \cdot (Packet\ Size)}{(CPU\ Speed\ (GHz))} \quad (5)$$

Additionally, for this model, it is assumed that the firewall equipment under consideration is the Cisco Firewall 4115 from the Cisco Secure Firewall 4100 Series Appliances (2023) data sheet. This firewall was chosen because Cisco is one of the largest technology companies and widely used in military networks. The 4100 series firewall model meets the team’s assumed bandwidth and security requirements. Based on the firewall datasheet, throughput values’ specifications were used to formulate Equation 6 to calculate the generated delay when a packet goes through a firewall. These values are pivotal in assessing the impact of the firewall on overall processing delay and network performance. The team also used these values to calculate the maximum throughput the network could handle as a resource pool. This information is essential for understanding how the firewall impacts network performance.

$$D_{Firewall} = \frac{(Packet\ Size\ (Bytes))}{(8Bytes)} \cdot 0.0035\ ms \quad (6)$$

The team used two fundamental equations to calculate the processing delay of data packets in the simulation mode. As a first step, the team used the firewall delay

equation, representing the time it takes for a data packet to traverse a specific firewall model. The equation was utilized to quantify the delay introduced by the firewall in the simulation. The team's model includes encryption delay equations that account for the time required to encrypt data packets using AES-256. Equation 7 sums the total value of the firewall delay and encryption delay equations. The team assessed the overall processing delay experienced by data packets in the simulation, providing valuable information regarding the network's performance.

$$D_{Processing} = D_{Firewall} + D_{Encryption} \quad (7)$$

(2) Serialization Delay

Serialization delay, a fundamental concept in data communication, quantifies the time needed to convert digital data into a format suitable for transmission over a constrained medium, for example a cable or a communication channel (Hac n.d.). This delay is a crucial consideration in networking and telecommunications, impacting data transmission efficiency and performance.

The magnitude of the serialization delay hinges on two key factors: the size of the data packet being sent and the channel's capacity through which it will be transmitted. To elaborate further, the relationship between these variables and the serialization delay is examined. Firstly, packet size plays a pivotal role in serialization delay. Larger packages require more time to serialize as they encompass more data that must be converted into the appropriate format for transmission. Conversely, smaller packets are processed faster in this regard. Secondly, channel capacity, which refers to the data transfer rate the channel can support, significantly influences serialization delay. A channel with a higher capacity transmits the data faster, thus reducing the serialization delay. Conversely, channels with limited capacity result in a longer serialization process. For instance, a 1.544 Mbps T1 line—a dedicated transmission connection between a service provider and client—is relatively modest compared to a high-speed 1 Gigabit (Gb) Ethernet connection, which boasts a significantly larger capacity.

To illustrate this further, the team compared the serialization delay for the same 1024-byte packet transmitted over these two channels. On a T1 line with a capacity of 1.544 Mbps, it takes approximately 5 ms to complete the serialization process for the 1024-byte packet (Oppenheimer 2011, chap. 2). In contrast, on a 1 Gigabit Ethernet connection, the serialization delay for the same packet is drastically reduced to a mere 1 microsecond (μs) (Oppenheimer 2011, chap. 5). This stark contrast demonstrates the profound impact of channel capacity on serialization delay.

The team made assumptions based on the Ethernet standard, a serialization delay of 1 μs was considered for the calculations as shown in Equation 8. This assumption allows for a simplified and consistent reference point, mainly when dealing with Ethernet-enabled networks and their respective channel capacities based on the network characteristics assumptions.

$$D_{\text{Serialization}} = 0.001 \text{ ms} \quad (8)$$

(3) Router Queue Delay

A router queue delay refers to the time elapsed between the time a packet arrives at a router queue and the time it starts the transmission process through the output link (Salehin and Rojas-Cessa n.d.). Unlike unavoidable network delays with precise formulas, router queue delay is contingent on the network usage state. It does not adhere to a fixed mathematical expression but exhibits a fluid nature influenced by multiple variables. Router queue delays can span a broad spectrum, ranging from just a few milliseconds to tens of milliseconds. This range is shaped by several factors, including the quantity of packets awaiting processing in the queue. It also includes the nature and type of network traffic and router processing speed.

The number of packets in the queue plays a pivotal role; when the queue becomes inundated with packets, it can lead to prolonged router queue delays. Furthermore, the type of traffic passing through the router also contributes to queue delay variability. Real-time, latency-sensitive traffic may have different effects on queue delays than less time-critical data. Lastly, the router's processing speed affects how quickly it can clear the queue, thus

affecting the delay. If router queue delays extend beyond an acceptable threshold, it can have significant repercussions, including traffic congestion and network degradation.

(4) Transmission Delay

Transmission delay, often called store-and-forward delay, represents the time required for all the bits comprising a data packet to be successfully loaded onto the network medium for transmission (Kurose and Ross 2013). This delay is a multifaceted phenomenon influenced by various factors, including the inherent latency of the network. It is also influenced by the speed of the transmission medium, and the processing delay incurred by the receiving device. The accumulation of these time intervals contributes to transmission delays.

Latency accounts for the time it takes for signals to traverse the network infrastructure, thus contributing to transmission delay. Additionally, the speed of the transmission medium, whether it is a cable, optical fiber, or wireless channel, can significantly affect how quickly data packets are conveyed. Slower transmission mediums naturally lead to longer transmission delays. Equation 9 provides the correlation between packet size and transmission rate to provide the transmission delay used in the simulation.

$$D_{Transmission} = \frac{(Packet\ Size\ (Bytes))}{(Transmission\ Rate(Bytes\ per\ ms))} \quad (9)$$

It is critical to note that excessive transmission delay can adversely impact network performance by impeding data flow speed, leading to reduced data transfer rates and potential bottlenecks in the network. Petroc Taylor (2023) documented empirical statistics of average transmission rates for Internet Service Providers (ISPs) which the team used in the model to gauge the average upload speed of 35.13 Mbps. This benchmark allows the team to estimate upload speed while considering transmission delay and the network infrastructure.

(5) Propagation Delay

Propagation delay refers to the time required for an electrical or optical signal to traverse the physical distance between two points within a transmission medium. This

delay is linked to the characteristics of the medium itself. Propagation delay can be influenced by a range of materials, from copper wires to advanced optical fibers. The nature of the medium profoundly influences the propagation delay, as signals propagate at varying speeds through different materials. Equation 10 sums up all the delay factors considered for both the fiber and copper wire networks.

$$D_{Total\ Propagation} = D_{FiberPropagation} + D_{CopperPropagation} \quad (10)$$

In network infrastructure and telecommunications, propagation delay is dependent on the transmission medium. For instance, the type of cable used can significantly affect propagation delay. Advanced optical fiber cables tend to exhibit lower propagation delay due to the high speed of light (c) in optical media, while traditional copper cables introduce higher propagation delay. This contrast underscores the importance of carefully selecting the transmission medium based on network requirements.

The model assumes a mixed medium environment where 95% of the transmission path utilizes fiber cables, known for their low propagation delay. The remaining 5% is composed of copper cables, introducing a slightly higher propagation delay. This distribution was primarily determined by aligning with the ISP test data, demonstrating that the team's choice was based on data. This hybrid approach allows for efficient data transmission while considering cost-effectiveness and other practical considerations. By considering the characteristics of the media, the model effectively incorporates propagation delay into the estimation of average upload speed for an ISP.

(6) Fiber Propagation

Optical fiber latency is a multifaceted parameter influenced by several critical factors. The refractive index of the optical fiber, the composition of its core material, and the length of the fiber all contribute to the overall latency experienced in data transmission. A comprehensive understanding of these variables is essential for accurately estimating optical fiber latency.

The refractive index of an optical fiber, a fundamental property, affects the speed at which light signals propagate through the medium. Higher refractive indices lead to

slower signal propagation, while lower indices facilitate rapid transmission. Similarly, the optical fiber core material significantly impacts signal velocity. Core materials are used based on their ability to guide light efficiently, reducing signal loss and distortion. Finally, the length of the optical fiber traversed by data signals plays a vital role in determining the total latency. Longer fibers introduce a greater latency as signals must cover a longer distance, encountering additional transmission delays. Equation 11 uses the length (L) of the fiber optic cable divided by the speed of light and multiplies it by the refraction index (n), assumed to be 1.47, to produce the fiber propagation delay (Carr, Saikkonen, and Williams 1990).

$$D_{Fiber\ Propagation} = \frac{L}{c} \cdot n \quad (11)$$

To ensure precise calculations of optical fiber latency, the model references sources such as the white paper, “Latency in Optical Fiber Systems” by Joseph Coffey (2017). This scholarly resource provides in-depth insights into the factors affecting latency within optical fiber systems, allowing for accurate and informed estimations. By leveraging this knowledge, the model achieves a more robust and realistic representation of optical fiber latency, a key component of network performance assessments.

(7) Copper Propagation

Copper transmission media latency is determined meticulously, involving specific parameters and underlying assumptions. These parameters and assumptions are also derived from Coffey (2017). This white paper serves as a valuable reference source that elucidates the intricacies of latency in both optical fiber and copper transmission systems.

Copper transmission media latency is dependent on a range of variables. These variables include the physical properties of the copper cable, the signal propagation speed through copper, and the distance over which signals must travel. Copper cables exhibit distinct latency profiles due to the comparatively slower propagation speed of electrical signals within copper conductors. The length of copper cabling, signal encoding, and any signal regeneration points along the transmission path can introduce additional latency variations. Equation 12 applies the length of the copper cable divided by 65% the speed of

light as explained by Coffey (2017). It is critical to emphasize that copper latency quantification is not solely theoretical; using real-world data and empirical measurements that have been methodically analyzed and documented.

$$D_{Copper\ Propagation} = \frac{L}{c * 0.65} \quad (12)$$

By relying on the insights from Coffey (2017), the model ensures that the latency values attributed to copper transmission media are well-informed and reflect practical realities encountered in network communication. This approach underpins network performance assessments' accuracy and reliability, particularly when copper-based transmission is used alongside other media.

(8) Fiber Transponders

Each time a fiber optic signal undergoes a conversion process, the network experiences an additional delay. This delay is a direct consequence of signal transformation's inherent complexities. The conversion typically occurs through a transponder, which alters the optical signal's wavelength. In practice, this means converting the signal from a short-range interoffice wavelength to a long-range wavelength using wavelength division multiplexing (WDM) technology and reverting it to its optical form.

In assessing these conversions, several assumptions come into play, each significant in estimating the overall delay. These assumptions revolve around the type of fiber employed, the operational range specific to fiber optic configurations, and the potential influence of data boost devices on latency. The team assumed a 5-kilometer (km) operational distance, based on the Institute of Electrical and Electronics Engineers (IEEE) (2008) Std 802.3-2008 Section 3, 36.1.2, before requiring a transponder on the fiber cable. Data boost devices—the transponders—introduce an incremental delay of 5 μ s at each retransmission point—every 5 km, as indicated in “Low Latency, How Low Can You Go?” (2020). Equation 13 accounts for the additional latency generated by each retransmission point for the total assumed fiber optic cable travel distance. Accounting for the added latency is essential as it can significantly impact the total delay in fiber optic

communication. In sum, these considerations and assumptions offer a comprehensive framework for evaluating and managing delays introduced during fiber transmission signal conversions, contributing to a more precise and realistic network performance model.

$$D_{Fiber\ Transponder} = \left[\frac{L * 0.95}{5\ km} \right] * 0.005\ ms \quad (13)$$

2. Simulation Model

To effectively model intricate network dynamics within the naval lab, the team recognized the necessity of simulation software that comprehensively represented various processes. The team identified ExtendSim as the software of choice due to its versatility and prowess in modeling complex systems that involve discrete events. This capability aligns with the discrete modeling approach for network data transfer (Imagine That 1987). ExtendSim is a robust and suitable solution for the network simulation needs of this project. It allows the team to simulate intricate interactions and processes within the network meticulously. Simulating the model in the ExtendSim discrete functionality enables the team to have a deeper understanding of network performance. It facilitates the development of more efficient operational strategies within the naval lab. The team used ExtendSim to help identify potential bottlenecks, optimize resource allocation, and enhance network efficiency. Its capacity to accurately replicate discrete events at specific time intervals ensures that the simulations closely mirror real-world network operations, aiding in the development and validation of strategies for improving network performance and reliability within the One Navy Lab's complex environment.

3. Simulation Model Assumptions

The following assumptions were made when creating the model.

Packet Generator:

- Network has a share bandwidth of 1 Gbps set as a resource pool in the model.

- The firewall in each lab has a maximum throughput of 40 Gbps, to match the assumption that the firewall configuration is set in the model as a resource pool.
- Packets are created using a schedule table in a constant stated format.
- A manual adjustment was made to the rate variation in order to meet testing requirements.
- There is an assumption that packets have a delay of 1 μ s between the creations of each packet. This procedure ensures that the software does not allocate the same attributes on a group of packets at the same time.
- Packets are assigned attributes which are predetermined and match the test requirements.
- Distance – Variance based on test scenario.
- Packet Size – 1500 bytes (matches MTU)
- Protocol Type – TCP or UDP
- Total Latency – 0 ms This is required to correct software generated errors.

Firewall and Encryption:

- Throughput limitations are based on Cisco Firewall 4115 hardware.
- The firewall latency is approximately 0.65625 milliseconds to mirror the constant packet rate of 1500 bytes.
- A 2.5 GHz CPU was used.
- An empiric table is used to generate the time value using a random number generator with a variance of 10%

Network Transmission:

- There is priority given to returning TCP packets over new packets sent to the router queue.
- Jitters are generated randomly using either ISP ping test data or an optimizer—which limits the maximum jitter to 30 ms.

Packet Receiver:

- Based on the random probability of failure based on ISP ping test data, 87.1% of the attempts are successful.
- A total latency of individual packets greater than 150 ms is considered a failure.

If the protocol is TCP:

- In the TCP protocol, the equation function will add an additional latency to the ACK packet.
- The ACK packet is assumed to be 46 bytes in size.
- A TCP packet is sent back to the router queue for resubmission instead of automatically being sent to the failure packet section.
- TCP packets will be resent until successful, and the failure factor is based on the total packet latency.

In the initial phase of the model, as seen in Figure 23 and in Appendix A, the simulation generates packets with a pre-determined time rate that represents the data transfer between systems. Each packet is endowed with various distinctive attributes, such as packet size, transmission distance, and protocol type. Once these attributes are defined, the packet undergoes a processing phase involving encryption and firewall-based transmission, guided by the assumptions. Upon completion of processing, the packet endeavors to secure available bandwidth resources. However, when no bandwidth is immediately available, the packet enters a queue element, symbolizing the router queue.

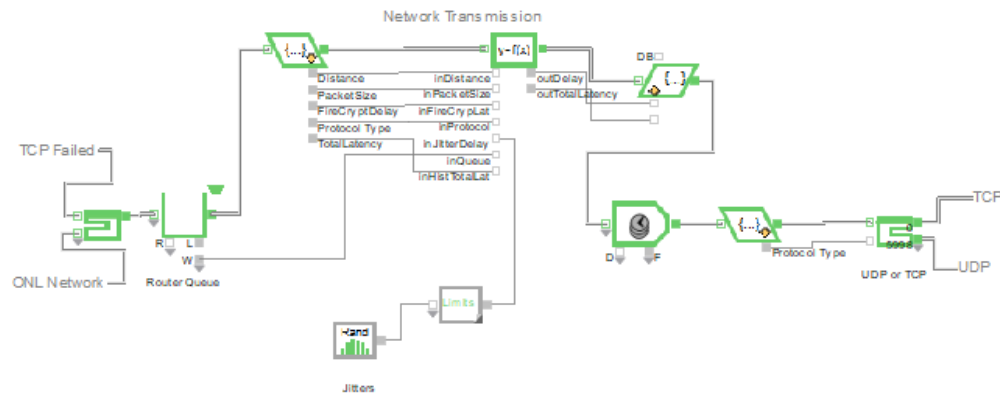


Figure 24. Network Transmission Section

In the final stage, the packet is decrypted and scrutinized through two critical assessments. First, the simulation performs a comprehensive evaluation to ascertain the likelihood of packet failure and determine whether it successfully reaches its intended destination. This assessment relies on probability-based analysis, accounting for packet failure within the planned network, using ping test data failure rates. If the packet protocol is UDP, the packet that is randomly determined to fail is forwarded to the Fail Packet section as shown in Figure 25 and in Appendix A. On the other hand, if the packet is using the TCP protocol, it will send the packet back to the network transmission section to resubmit the packet as its intended operation of the TCP packets, shown in Figure 26 and in Appendix A. Second, the team assessed whether the total latency time exceeds the designated threshold of 150 ms, which indicates potential issues. These steps collectively constitute a comprehensive and detailed simulation of the packet's journey through the web. The team used this model to analyze the data transfer processes.



4. Simulation Analysis

The central objective of the simulation study involves conducting distance and data rate tests to understand the critical factors that influence the success of data packet transmission between two laboratories. In the realm of network communication, it is essential to comprehend what drives the efficiency and reliability of data exchange. The distance and data rate tests offer insights into the dynamics of this process and shed light on the intricacies of laboratory network performance.

The distance test is a pivotal component of the analysis. The distance test is only dependent on distance and protocol type—UDP or TCP. The results show the percentage of packets that successfully reached the destination and under 150 ms of latency. This test encompasses a simulation that runs for one minute. The packet size employed in this test is 1,500 bytes, tailored to match the MTU value. Moreover, a constant data rate of 300 kilobytes per second (kBps) is maintained throughout the test. To account for network latency introduced by firewalls and encryption processes, Equation 6 was implemented. The test was conducted at a variety of distances, ranging from 1 km to 9700 km, mirroring the possible network configurations between laboratory locations within the U.S.

Figure 27 shows the distance test results using the ISP jitter for TCP and UDP. Initially, TCP started at a success rate of 94.0%, while UDP had a success rate of 82.7%. As the distance traveled increased, both protocols exhibited a consistent decline. UDP shows a controlled decline of less than 0.88% between each distance, spanning a distance from 1 km to 8900 km, after which a notable drop of 1.66% is observed. In contrast, TCP shows a steady decrease of less than 0.44% between each distance through 3200 km, after which the packet success rate started decreasing by 1.30% between each distance. After 4800 km, the packets success dropped drastically from 90.0% to 81.0% and lower. This shows that after 6400 km, TCP is as reliable as UDP.

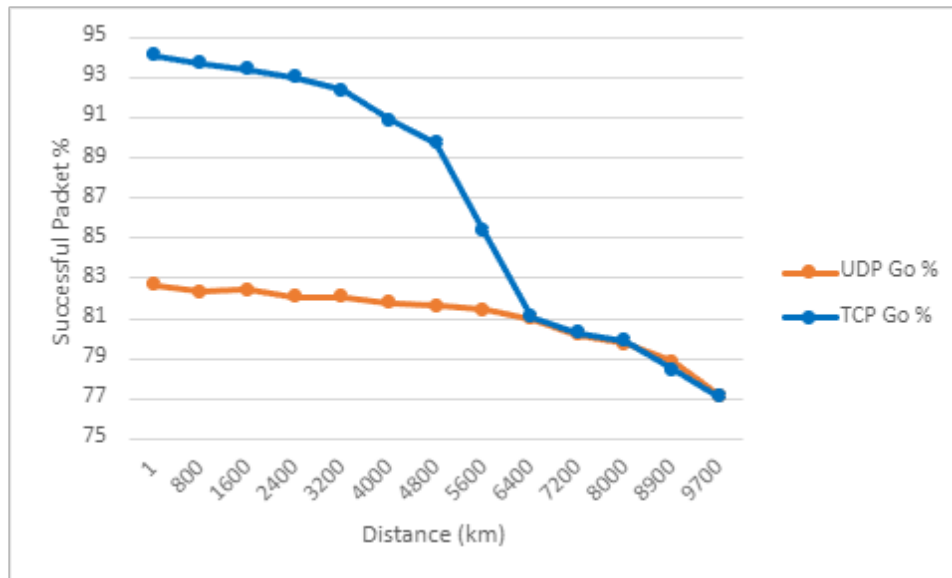


Figure 27. Distance Test with Internet Service Provider (ISP) Jitter

Figure 28 shows the results of a distance test with optimized jitters. TCP initiates with a 100% success rate, and in comparison, UDP initiates with an 87.0% success rate. This shows that optimizing jitters has a positive impact on the packet success rate. Both show a consistent decline as packets' distance traveled from the source increases. UDP packets demonstrate a controlled decline of under 0.02% between each distance, from 1 km to 7200 km, after which the drop increases to 7.11%, and then decreases to an average of 1.31% between each distance. In comparison, TCP exhibits a slight drop of 0.38% up to 3200 km, after which the decline accelerates to an average of 2.83% until 6400 km. It can be seen starting from the distance of 6400 km, both UDP and TCP behave the same.

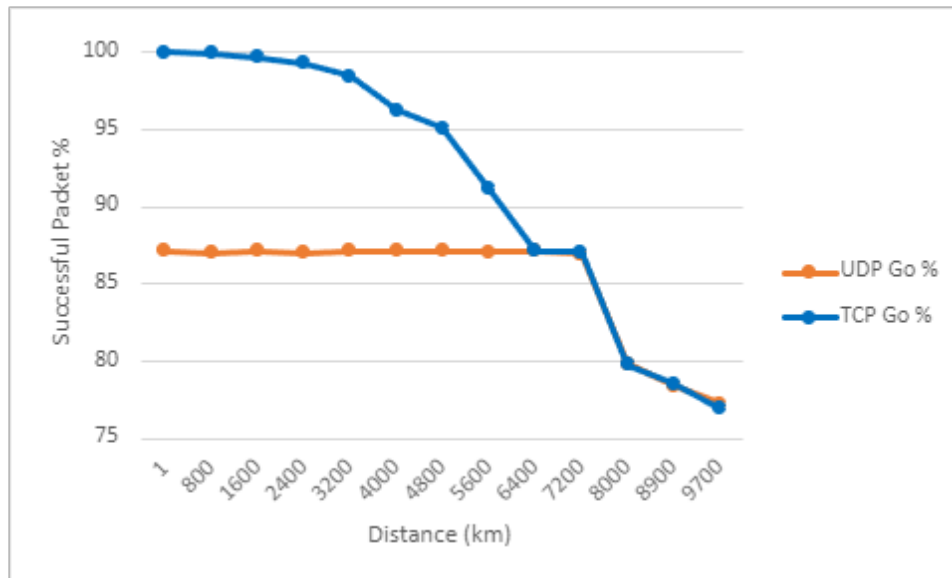


Figure 28. Distance Test with Optimal Jitters

The data rate test shares similarities with the distance test in terms of test duration, of one minute and packet size of 1,500 bytes. This test is conducted at one distance but with varied data rates to show how the amount of data pushed through impacts how many packets successfully reach their destination under the 150 ms latency requirement. The firewall delay is consistent with assumed hardware configuration, while the AES-256 calculation accounts for the 2.5 GHz CPU speed variations with a random 10% fluctuation. Figure 29 shows that neither UDP nor TCP exhibit fluctuations until 20% of the bandwidth is used. Based on the 1 Gbps (1,000 Mbps) bandwidth, it is assumed that 200 Mbps represents 20% bandwidth utilization. Once this threshold is exceeded, TCP experiences a decline in successful packet delivery, dropping from 77.0% to 22.0%. As a result of this analysis, it can be concluded that the type of transmission protocol used may limit the maximum data rate that the network can handle in a constant state. If a higher data rate is required, the bandwidth of the network must be optimized (by reduction of network jitters and packet loss) or additional network management procedures must be established to accommodate the increased demand. Additionally, network performance may also suffer from network congestion, which can be caused by the number of devices connected to the same network.

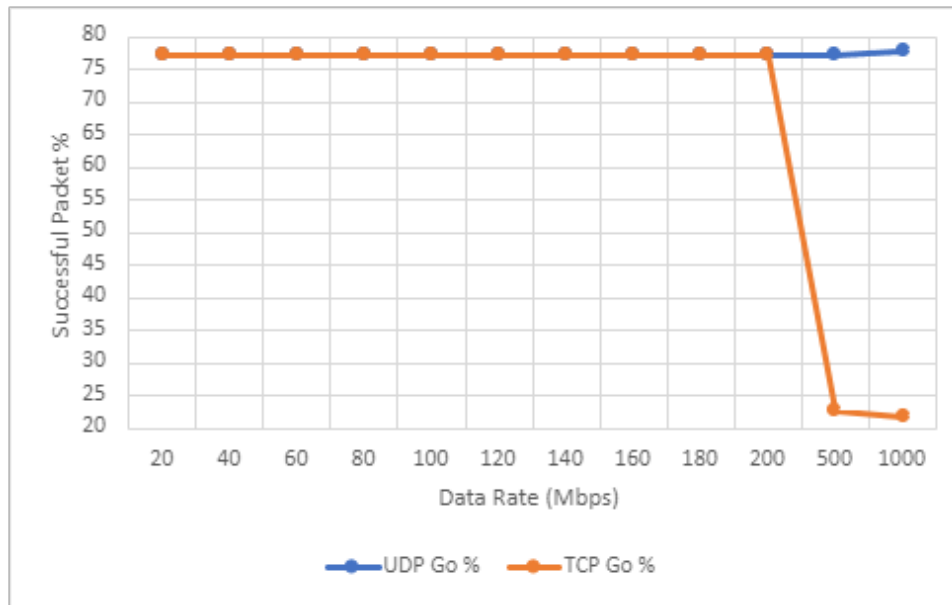


Figure 29. High Data Rate Test at 9700 km

The analysis of the test results reveals significant insights into network performance. Factors such as distance and jitter emerge as influential determinants. The distance test unveils that the success rate of data packets remains consistent up to 3200 km, both when using ISP and optimized jitter distances. Once the distance reaches 6400 km, the success rate declines similarly regardless of protocol (UDP/TCP). During the high data rate test, the UDP protocol demonstrated minimal variation in its overall success rate, while the TCP protocol experienced significant changes. The point at which TCP begins to exhibit negative effects can be reduced by reducing laboratory distance and network quality, i.e., decreasing jitter and packet failure, resulting in a shorter round-trip time for packets. By doing this, the network would be able to release bandwidth at a faster rate, thus improving bandwidth utilization.

Considering these findings, the team drew several conclusions. Depending on the specific network requirements of stakeholders, it is recommended to consider alternative solutions for laboratory locations separated by more than 3200 km. Beyond this threshold, a pronounced increase in packet failures is observed. However, it is imperative to emphasize that improving network quality, minimizing jitter, and dealing with packet failures within the network can potentially extend the effective distance. The improvement

of network performance involves prioritizing packets, minimizing unnecessary bandwidth usage, checking your device frequency, and scheduling online activities to minimize conflicts. Based on the analysis performed in this section, the results will support the Earned Value evaluation in Chapter VIII.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. VERIFICATION AND VALIDATION

This chapter examines the V&V processes for the One Navy Lab framework development using the Validation Square, a process specifically designed to evaluate engineering design methods (Pedersen et al. 2000). The One Navy Team's methods of evaluation of feasibility, effectiveness, and economy are assessed. This chapter offers insights into the strengths and weaknesses of the methods used and provides suggestions for improvement.

A. V&V ANALYSIS

V&V are processes used to determine if a system meets its requirements. Verification is confirming that the system follows its system-level requirements or specifications and justifying whether it was built correctly (National Aeronautics and Space Administration [NASA] n.d.). It can be performed at any stage of the system life cycle; however, it is commonly used during the development stage. Validation is a quality assurance process to determine if all the requirements are met by proving that the right system or product was built (NASA n.d.). Validation is usually performed during or after the integration of the system, under realistic conditions, to determine if the stakeholders' objectives are met. During the process, any defects or anomalies discovered need to be resolved before final delivery. Verification confirms the approved requirements, while validation confirms the MOEs, MOPs and CONOPS (NASA n.d.). Even though there are four methods for completing a V&V (testing, inspection, demonstration, and analysis), testing is a requirement to validate the end-product.

B. THE VALIDATION SQUARE

The Validation Square is a comprehensive process designed to instill confidence in the research's usefulness, particularly in design methods. According to Pedersen et al., the Validation Square involves "evaluating the effectiveness and the efficiency of a method, based on qualitative and quantitative measures respectively" (Pedersen et al. 2000, 5). The qualitative and quantitative measures are distributed over four squares, theoretical

structural, empirical structural, theoretical performance, and empirical performance validities, as seen in Figure 30.

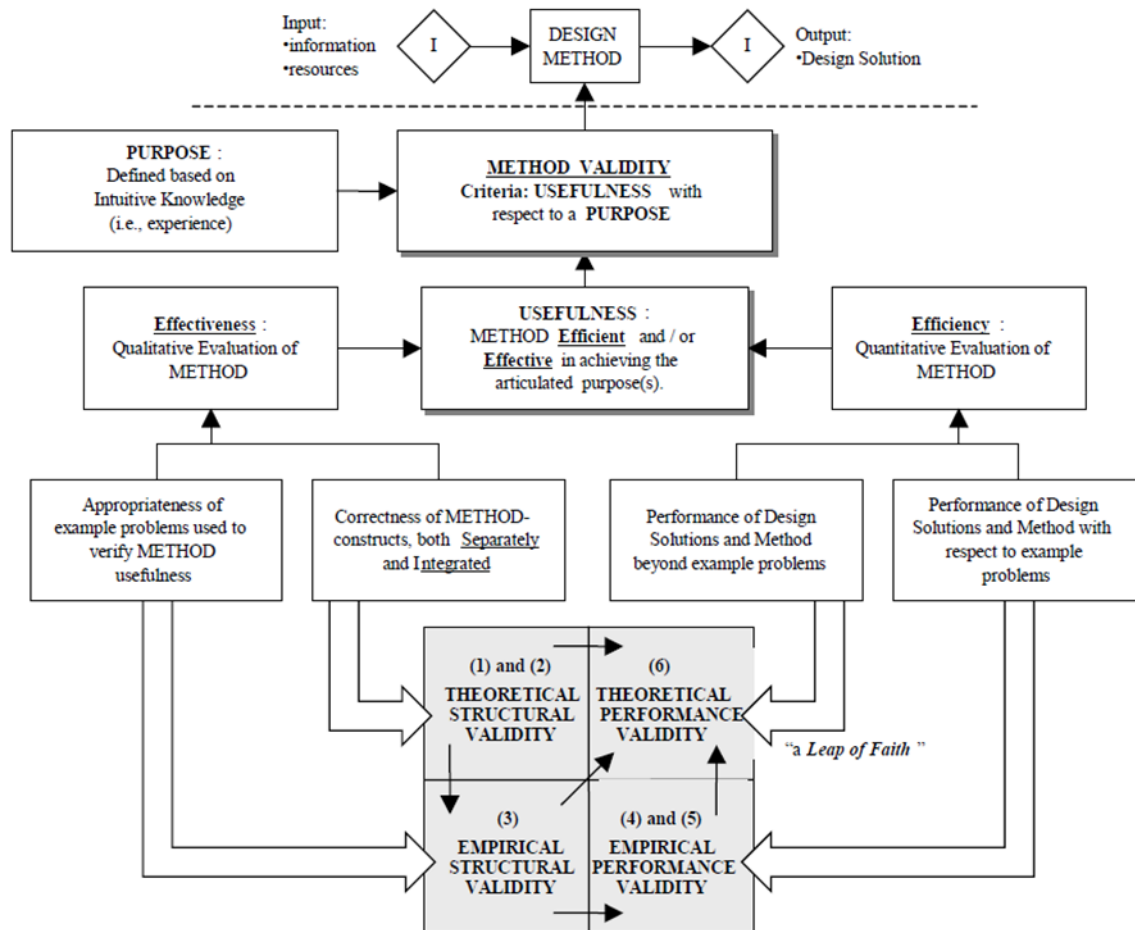


Figure 30. Validation Square. Source: Pedersen et al. (2000).

Structural validity refers to accepting the method's individual constructs, accepting the consistency of integration of the constructs, and proving their conceptual soundness with example problems (Pedersen et al. 2000). Structural validity can be broken down into three steps embodying the first two squares. Pedersen et al. (2000) detail the first square, theoretical structural validity, as involving accepting the validity of individual constructs through literature analysis and ensuring internal consistency through flow-chart representations. The second square, empirical structural validity, is to build confidence that the example problems are suitable for specific cases (Pedersen et al. 2000). In contrast to

structural validity, which focuses on effectiveness, the theoretical and empirical performance validity focuses on efficiency. The performance validation processes make up the remaining two squares; the third square includes evaluating the method's usefulness with selected example problems, and the fourth square includes linking the achieved usefulness in those example problems to the application of the method and establishing its utility beyond a specific set of circumstances (Pedersen et al. 2000). As a result, the Validation Square is a process for building confidence in a design method's general applicability and effectiveness.

The context and importance of the Validation Square process are vital to the development of this report. The Validation Square provides integrity to assumptions, research, analysis, and recommendations made and completed in the One Navy Lab conception. Development of a One Navy Lab is complex in the way in which various components must interact to support the use cases developed in Chapter IV, so the Validation Square supports the processes used to identify and analyze the various One Navy Lab COAs. The Validation Square provides a structured and logical approach for evaluating the effectiveness of different engineering analysis methods in the development of the COAs. Using the Validation Square allowed the team to ensure that the chosen solutions logically aligned with the stakeholders' needs and requirements.

1. Theoretical Structural Validity

The first step in the Validation Square process is the theoretical structural validity of the evaluation of each COA. This involves examination of the relationships between the COAs and examples of similar existing operations that also meet the stakeholder requirements. Ultimately, the theoretical structural evaluation validates that the objectives of the COAs are achieved.

a. COA 0 – Status quo

COA 0 represents the current working setup for integration and interoperability testing on board ships. Engineers also travel to various LBTSs for other combat systems taskings. As this COA is the current way of operations, it is proven to successfully support the use cases the One Navy Lab is required to satisfy.

COA 1- A land-based test site

The similarity between COA 1, a fully integrated LBTS, and the Combat Systems Engineering Development Site (CSEDS)—an LBTS located in New Jersey—lies in the shared objective of creation of a controlled environment for testing and advancing combat systems. Like CSEDS, where combat element systems are integrated and tested on land, COA 1 envisions a comprehensive lab that mirrors and expands on CSEDS capabilities to include a fully shipboard representative combat system. Naval Station Norfolk is the Navy’s largest naval installation, stretching up to 11 km (pier and wharf distance) and it is unlikely that the size of the facility will impact the operations of the systems due to the speed at which data travels (Commander, Navy Region Mid-Atlantic [CNRMA] n.d.). Given that CSEDS and COA 1 are similar in functionality and configuration, the requirements in Table 8 met by CSEDS is also assumed to be met by COA 1. Thus, COA 1 can confidently provide the same benefits as CSEDS in terms of testing combat systems.

b. COA 2- Multiple Land-Based Test Sites

COA 2 is a multiplicity of COA 1, which was introduced to evaluate the elimination of temporary duty (TDY) costs. COA 2, which aims to establish a fully integrated combat systems lab at each warfare center, will operate in a similar manner to COA 1. Similarly, current operations show CSEDS and Surface Combat Systems Center (SCSC) are both naval combat systems LBTSs, located in New Jersey and Virginia, respectively, and are supporting naval testing and taskings. As COA 2 is similar to the multi-lab set up, currently in operation, which meets the requirements in Table 8, an assumption can be made that COA 2 meets all the requirements also.

c. COA 3- Connects Separate and Independent Labs Using a Naval Network

To encourage a net-centric collaborative environment, as described in the JIE strategy, the team evaluated COA 3—the connection of separate and independent weapon labs using a naval network. As the configuration of this COA has not been implemented previously, the team used modeling and simulation to evaluate the feasibility of this alternative. The primary difference between this COA and the other alternatives is the physical distance between each system. This distance could impair requirement 2.1, which

necessitates that the interface requirements of the combat systems elements are met. Requirement 2.1 is decomposed into key performance parameters, as seen in Table 11, which dictates if requirement 2.1 is met. Hardware and software configuration in the labs and the network infrastructure will determine whether the bandwidth's KPPs are met. DOD networks are maintained to be ahead of DOD technology requirements; thus, the team assumed the NOLIN network has a 1 Gbps connection which exceeds operational bandwidth requirements. The jitter requirement of 30 ms or less is also assumed to be met, as the DOD networks are continuously monitored to upkeep quality of service. The team evaluated the COA's latency requirements against the hard real-time (1ms) and the soft real-time (150ms) requirements, as seen in Table 9, to ensure that each of the use cases can be completed.

2. Accepting Method Consistency

Within this decision-making process, as shown in Figure 31, data flow begins with the following inputs: COAs, which represent potential strategies; verification plans, which detail the process and resources that will be used to ensure compliance; requirements, such as low-level specifications or KPPs; and resources, such as simulations and models. After receiving these inputs, several methods are used to process them strategically. First, mission analysis ensures alignment with project objectives and verifies feasibility of the COAs. This is followed by a comprehensive review, considering the COA requirements, costs, and risks. Analyzing the results involves assessing results, which are influenced by the performance of the COA and guided by the verification plan. Finally, preparing the system verification report consolidates verification outcomes and modeling data. As a result, stakeholders will receive informed recommendations that provide a comprehensive view of the COAs, requirements, costs, and risks. This will enable stakeholders to make decisions aligned with the project's mission.

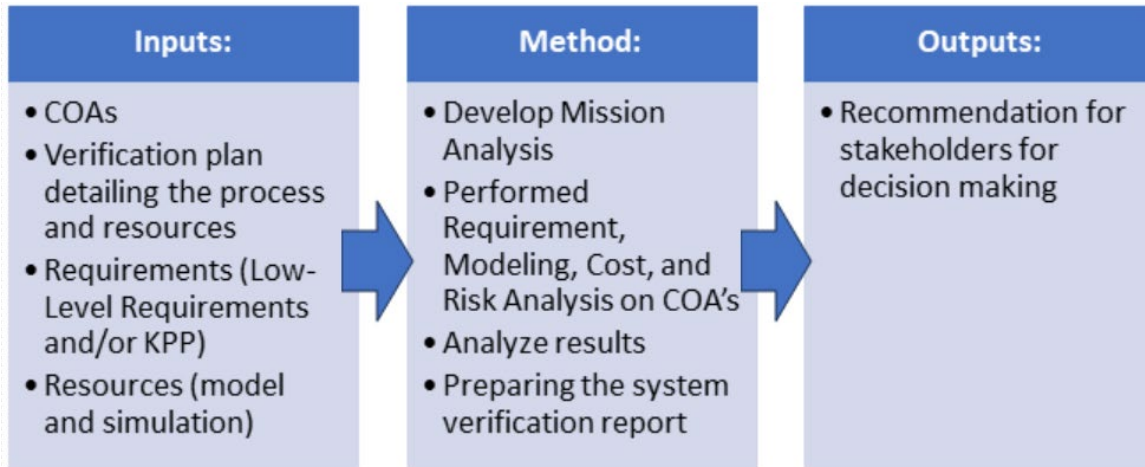


Figure 31. Method Internal Consistency Information Flow

The following methods reflect a systematic approach to decision-making: Mission Analysis, Requirement Modeling, Cost Analysis, Risk Analysis, Analyzing Results, and Preparing a System Verification Report. These methods are instrumental in developing and managing projects in various fields. For a better understanding of how each method contributes to the development of the stakeholder recommendations, each approach is examined individually:

Mission Analysis:

- Purpose: Establishing clearly defined goals and objectives for the project.
- Validity for Stakeholder Recommendation: By understanding the mission, the project can be aligned with stakeholder expectations. For stakeholders to make informed decisions, they must clearly understand the project's purpose and how it aligns with their interests.

Modeling Analysis:

- Purpose: Identify, document, and analyze the COA 3 network behavior, since there is no equivalent system currently available that can provide a feasibility assessment.

- **Validity for Stakeholder Recommendation:** Stakeholders need to be aware of the project's requirements to ensure that the final product meets their needs. Requirement modeling helps in visualizing and communicating these requirements, making it easier for stakeholders to provide input and make decisions.

Cost Analysis:

- **Purpose:** To estimate the financial resources required for the project.
- **Validity for Stakeholder Recommendation:** Stakeholders, especially those responsible for budgeting and financing, need to understand the costs involved. Cost analysis provides the necessary information for stakeholders to make decisions based on financial considerations.

Risk Analysis:

- **Purpose:** To identify and assess potential risks that could impact the project.
- **Validity for Stakeholder Recommendation:** Stakeholders must be aware of potential risks and uncertainties. Risk analysis allows stakeholders to understand the possible challenges and make decisions on risk mitigation strategies. This ensures that decision-makers are well-informed about potential obstacles and can plan accordingly.

Analyzing Results:

- **Purpose:** To evaluate the outcomes of the project or system development process.
- **Validity for Stakeholder Recommendation:** Analyzing results provides stakeholders with insights into the project's performance, success, and areas for improvement. This information is crucial for making recommendations and decisions about the future direction of the project.

Preparing System Verification Report:

- Purpose: To document and communicate the verification process and outcomes.
- Validity for Stakeholder Recommendation: Stakeholders need assurance that the system meets the specified requirements. The verification report provides a comprehensive overview of how well the system aligns with the established criteria, helping stakeholders make recommendations based on the system's performance and compliance.

In summary, each method plays a specific role in the project or system development life cycle. By systematically employing these methods, stakeholders can gain a comprehensive understanding of the project, its requirements, costs, risks, and outcomes. This information forms the basis for informed decision-making and recommendations that align with the overall objectives and expectations of the stakeholders.

3. Empirical Structural Validity

Implementing the decision-making process, mainly through methods such as developing mission analysis, performing requirement modeling, analyzing the cost and risk of the COAs, analyzing results, and preparing the system verification report, introduces several challenges with human error emerging as a significant concern. Individuals performing complex analytical tasks and interpreting multifaceted data can lead to mistakes. Figure 32 illustrates the methodology used by the One Navy Team from development of stakeholders' requirements to analysis of COAs against the requirements to prove a recommendation. Methods utilized by the team to mitigate errors in developing the stakeholder's recommendations are also explained.

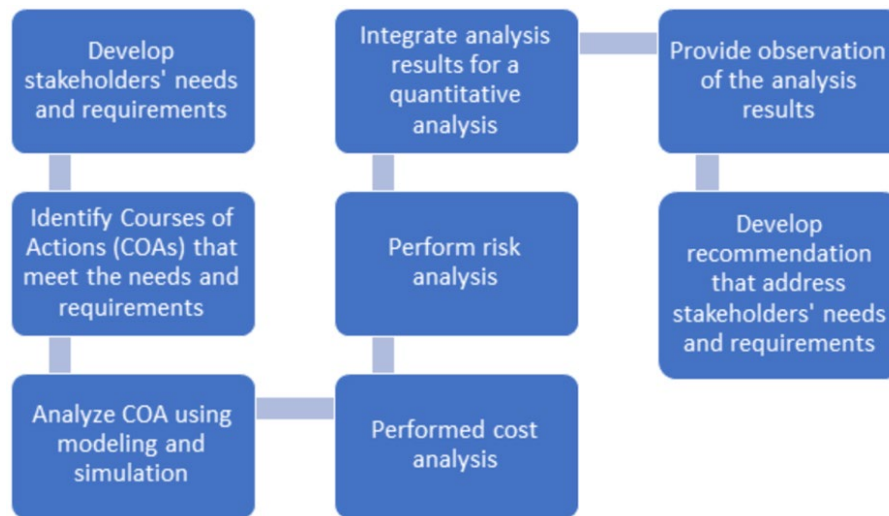


Figure 32. Methods to Develop Stakeholders' Recommendations

a. Verification of Development of Stakeholder Needs and Requirements

In the development process of the One Navy Lab, the stakeholders' needs and project objectives must be aligned correctly. It was accomplished by meticulously establishing traceability between higher-level project objectives and detailed requirements. To achieve clear and transparent connections between stakeholders' needs, requirements, and project goals, each requirement was systematically linked to its originating stakeholders' needs or project objectives. As a result of this traceability, not only did the development team have a comprehensive roadmap, but it also served as a robust verification system.

b. Verification of COA Identification

The team adopted a strategy of internal discussion and assessment to minimize human error during the identification of the COAs. By facilitating an open and collaborative environment, team members utilized diverse perspectives and expertise to examine potential COAs thoroughly. As a result of internal discussions, team members shared knowledge, challenged assumptions, identified potential pitfalls, and refined the proposed COA together. Each member contributed their unique insight with their distinct roles and responsibilities within the team, reducing the likelihood of oversights or cognitive biases.

c. Verification COA Analysis Using M&S

The team used unit testing to verify the various parts of the model. This ensured they were consistent with the assumptions and formulas used in their development. To ensure that each component of the ExtendSim application was consistent with the underlying assumptions and mathematical formulations employed in its development, the team implemented this testing approach. This type of testing was conducted due to the compartmentalized functional block design allowing each component to be meticulously verified. The team aimed to improve the model's accuracy and reliability through this systematic unit testing process. This ultimately contributed to its overall robustness and effectiveness.

d. Verification Integrated Analysis Results

To minimize errors during the development of integrated analysis, the team prioritized internal reviews as a critical quality control method. Members of the team conducted regular internal reviews in which they meticulously examined the various components of the analysis, including data inputs, methodologies, and interpretation of results. Collaboration and iteration facilitate the identification and correction of potential errors or inconsistencies before the final product is produced.

e. Verification of Risk Analysis

During the risk analysis development, the team used DOD guides to develop the section. The team evaluated the risks and identified potential mitigation strategies for each COA in different scenarios. The likelihood of each risk and its consequence occurring were determined. Both the likelihood and risk levels were appropriately cross-referenced with the DOD risk analysis guides. To minimize biases, the team used internal reviews using historical precedence when determining the different scenarios.

f. Verification of Performance Cost Analysis

The team performed a literature review to guide the cost analysis by examining established weapon systems as examples. This enhanced the accuracy and reliability of performance cost analysis. By reviewing the literature, the team gained a better

understanding of existing weapon systems and the costs associated with them. Additionally, collateral costs such as TDY were also understood and established. As a result, a more accurate and reliable cost analysis was developed.

g. Verification of Observation Analysis

In the observation analysis, the team analyzed one another's research and analysis and documented the results and patterns observed. The team then compared notes and cross-referenced conclusions. This approach reduced bias risk and conclusion error, by eliminating single point of view observations, which strengthened the reliability of the drawn conclusions.

h. Verification of Developed Recommendations

In the process of developing stakeholders' recommendations, the team developed recommendation evaluation methods, such as EV and the weighted evaluation matrix. Frequent internal reviews identified potential errors or oversights to these evaluation datasets. The team used tools, such as Excel, to develop these evaluation instruments; the tools' internal error-checking functionality supported human error elimination. Using this approach enhanced the reliability and accuracy of the recommendation development process.

4. Empirical Performance Validity

In applying the Validation Square methods meticulously, the team seamlessly integrated qualitative and quantitative approaches, providing stakeholders with an analysis that addresses their specific needs and requirements. The use of qualitative methodologies, used on the requirement analysis, provided valuable insights into the non-measurement aspect of stakeholders' needs. The team also utilized robust quantitative methodologies to analyze the input data, including risk analysis, cost analysis, simulation and modeling. A quantitative weight matrix was developed using qualitative evaluating factors to facilitate selecting a recommended COA. This comprehensive strategy ensured that both the qualitative nuances and quantitative insights were considered, fostering a more holistic reasonable recommendation.

5. Future Validation Square Assessment

In the Validation Square, steps 5 and 6 are “Accepting that usefulness is linked to applying the method,” and “Accepting the usefulness of method beyond example problems” (Pedersen et al. 2000, 7). These steps, part of the empirical and theoretical performance validity, respectively, are quantitative evaluations conducted for a concept that is further developed. As such, the team recommends these two steps as future work once the designs are developed and can be tested for accurate quantitative values.

VIII. COST AND RISK ANALYSIS

The team conducted a cost analysis to estimate the cost of the various COAs. A risk analysis was also completed to identify the major risks of the systems and their mitigation plans. This chapter presents both the cost and risk analyses.

A. COST ANALYSIS

DOD's past contract awards related to LBTSs and past budgets for testing environments were used to estimate the cost of the various COAs. The following assumptions were made:

- The time to perform the tasks of each use case is the same for each COA.
- Four warfare centers are part of the One Navy Lab.
- Each warfare center completes eight TDY per year.
- Each TDY takes four weeks to complete.
- Two personnel participate in each TDY.
- The labor rate is \$220 per hour.
- It takes six months for one full time personnel to obtain an ATO for a Zone D lab.
- It takes 12 months for one full time personnel to obtain an ATO for a Zone B lab.
- The life-cycle period of each COA is nine years.

1. COA 0 Cost

COA 0 accumulates high recurring costs from TDY travel, which are estimated to cost each warfare center approximately \$155,000 per year. The average cost of TDY was obtained by taking the average of the TDY cost from PHD to Norfolk, PHD to Pearl

Harbor, PHD to San Diego and PHD to Indian Head. The assumptions made when calculating the costs for each location are presented in Appendix B. COA 0 has a recurring cost of \$155,000 per year for each warfare center, which totals to \$620,000 per year for four warfare centers.

2. COA 1 Cost

This COA has both recurring and non-recurring costs. The non-recurring cost comes from the set-up of one fully integrated lab, which includes building a facility, and purchasing and installing the required hardware and software. In 2023, a land-based test facility for DDG was built in Philadelphia at a cost of \$122,000,000 (LaGrone 2023). The team assumes that the DDG LBTS's estimate can be applicable to COA 1 and that approximately \$122,000,000 is required to build the lab. The recurring cost for COA 1 is from meeting the cybersecurity requirements and the TDY cost for traveling to the lab. COA 1 requires an ATO for a Zone D lab. Based on the requirements for a Zone D lab, it is assumed that obtaining an initial ATO for a Zone D lab takes six months for one full-time personnel. Therefore, at an hourly rate of \$220, the cost of getting an initial ATO for a Zone D lab is approximately \$211,200. A reauthorization needs to be obtained every three years at the same cost of \$211,200. Additionally, the RMF requires continuous monitoring of the system, which is estimated to be half of the authorization cost, \$105,600, for each year that reauthorization is not required. Therefore, the cost of maintaining the ATO can be estimated at \$422,400 for every three years. Moreover, COA 1 has a recurring cost from traveling to the lab. As for COA 0, the TDY cost of COA 1 is estimated to be \$155,000 per year. As a result, COA 1 has an initial cost of \$122,211,200 for building the facility and obtaining the initial ATO, a recurring cost of \$422,400 every three years for maintaining the ATO, and a recurring TDY cost of \$155,000 per year for each participating warfare center. If four warfare centers are part of the One Navy Lab, the TDY cost is approximately \$620,000 per year for all four warfare centers.

Each warfare center can also estimate how the scheduling conflicts, caused by sharing the lab among multiple efforts at the same time, affect the schedule of the projects and their budgets. Planned value (PV), defined as “budgeted cost for work scheduled,” is

estimated to be the total project cost multiplied by the percentage of planned work (EcoSys 2022). The warfare centers can calculate the PV of each project to estimate the cost of the scheduled work. Earned value (EV), also known as “budgeted cost for work performed,” is estimated by multiplying the total project cost with the percentage of actual work completed (EcoSys 2022). EV should be utilized by each warfare center to calculate the actual cost of the work performed. Schedule variance (SV), an indicator of divergence from planned schedule, is estimated as the EV minus PV. Being behind schedule and possibly over budget is shown by a negative SV, being ahead of schedule and possibly under budget is shown by a positive SV, and being on schedule and possibly on budget is shown by a zero SV (EcoSys 2022).

For example, a situation can exist in which the shared lab is in Dahlgren and both PHD and Dahlgren are planning to use the lab the same week. The schedule conflict is discovered just a few days before the scheduled week and Dahlgren ends up using the lab instead of PHD. PHD planned to complete a week of testing at a budget of \$10,000. The PV for the test will be \$10,000 (calculated by $\$10,000 \times 100\%$ of planned work), while its EV will be \$0 (calculated by $\$10,000 \times 0\%$ of completed work). As a result, PHD will have an SV of $-\$10,000$ (calculated as $\$0 - \$10,000$) indicating that the test is behind schedule. If the conflict occurred at the end of the FY, then it will be difficult to obligate the extra money before it expires.

By comparing the PV and EV and calculating each project’s SV, the warfare centers will be able to determine if there was a schedule slippage that affected completing the project on time and staying on budget. If a schedule slippage occurs, the source of it should be determined and mitigation strategies should be created and implemented for future works.

3. COA 2 Cost

COA 2 accumulates costs associated with the set-up of duplicate labs, including building facilities, purchasing and installing hardware and software, and meeting cybersecurity requirements. As in COA 1, setting up one fully integrated lab is estimated to cost around \$122,000,000. Therefore, it is estimated that approximately \$488,000,000

is required to build the labs for four warfare centers. COA 2 has a recurring cost from obtaining and maintaining an ATO for the Zone D labs. As in COA 1, the cost of getting an ATO for a Zone D lab is approximately \$211,200 for one lab. Therefore, acquiring ATOs for the four labs is estimated to cost \$844,800. In addition to the initial ATO cost, reauthorization is needed every three years at the same cost of \$211,200 per lab, \$844,800 for the four labs. Additionally, the continuous monitoring of the system is estimated to be half of the authorization cost, \$422,400 for four labs, for each year that reauthorization is not required. Therefore, the cost of maintaining the ATO can be estimated at \$1,689,600 every three years for four labs. As a result, COA 2 has an initial cost of \$488,844,800 and a recurring cost of \$1,689,600 every three years.

4. COA 3 Cost

Most of the networks that COA 3 can use are available in most locations and they incur no network operations and equipment costs as they are covered by an external agency. Requesting to add additional nodes to a location is also covered by the external agency, up until the agency runs out of funding. At that point, the requester can wait until next year to get the nodes agency-funded or pay approximately \$50,000 for JIOR or \$88,000 for JMN to get the nodes installed. An assumption is made that getting an initial ATO for a Zone B lab requires double the effort of getting an ATO for a Zone D lab due to the added firewall and encryption security controls of adding a network to the lab. Since it takes six months to get an ATO for a Zone D lab, an ATO for a Zone B lab will require twelve months of work for one full-time personnel. Therefore, with an hourly rate of \$220, the cost of getting an ATO for a Zone B lab is approximately \$422,400. In addition to the initial cost of obtaining an ATO, reauthorization is required every three years at the same cost of \$422,400. Additionally, the continuous monitoring of the system is estimated to cost \$105,600 for each year that reauthorization is not required. Therefore, the cost of maintaining the ATO can be estimated at \$633,600 every three years. As a result, COA 3 has an initial cost of \$422,400 for obtaining an initial ATO and a recurring cost of \$633,600 every three years for maintaining the ATO, per warfare center. If four warfare centers are part of the One Navy Lab, the cost of COA 3 is approximately \$1,689,600 for the initial cost of the ATOs and \$2,534,400 every three years for maintaining the ATOs.

5. Cost Comparison

Cost comparisons were completed to identify the most cost-effective COA. The price differences presented in Tables 12, 13, 14, and 15 were calculated for the first year, third year, sixth year, and ninth year after the implementation of the COA. For the comparison, the team assumed that all four warfare centers used the same COA. The differences between COAs were calculated by taking the value in the first column (green cell) minus the value in the first row (red cell). For example, in Table 12, the difference between COA 0 and COA 1 was calculated by taking the value of COA 0 (\$620K) minus the value of COA1 (\$122.8M) resulting in a value of -\$122.2M. This means that COA 0 costs \$122.2M less than COA 1.

Table 12. Cost Comparison during the Implementation Year

Cost of COAs	COA0 \$620K	COA1 \$122.8M	COA2 \$488.8M	COA3 \$1.7M
COA0 \$620K	\$0	(\$122.2M)	(\$488.2M)	(\$1.1M)
COA1 \$122.8M	\$122.2M	\$0	(\$366M)	\$121.1 M
COA2 \$488.8M	\$488.2M	\$366M	\$0	\$487.1M
COA3 \$1.7M	\$1.1M	(\$121.1M)	(\$487.1 M)	\$0

Table 13. Cost Comparison Three Years After the Implementation

Cost of COAs	COA0 \$1.9M	COA1 \$124.5M	COA2 \$490.5M	COA3 \$4.2M
COA0 \$1.9M	\$0	(\$122.6M)	(\$488.7M)	(\$2.4M)
COA1 \$124.5M	\$122.6M	\$0	(\$366M)	\$120.3 M
COA2 \$490.5M	\$488.7M	\$366M	\$0	\$486.3M
COA3 \$4.2M	\$2.4M	(\$120.3M)	(\$486.3 M)	\$0

Table 14. Cost Comparison Six Years After the Implementation

Cost of COAs	COA0 \$3.7M	COA1 \$126.8M	COA2 \$492.2M	COA3 \$6.8M
COA0 \$3.7M	\$0	(\$123.1M)	(\$488.5M)	(\$3.1M)
COA1 \$126.8M	\$123.1M	\$0	(\$365.4M)	\$120 M
COA2 \$492.2M	\$488.5M	\$365.4M	\$0	\$485.5M
COA3 \$6.8M	\$3.1M	(\$120M)	(\$485.5 M)	\$0

Table 15. Cost Comparison Nine Years After the Implementation

Cost of COAs	COA0 \$5.6M	COA1 \$129.1M	COA2 \$493.9M	COA3 \$9.3M
COA0 \$5.6M	\$0	(\$123.5M)	(\$488.3M)	(\$3.7M)
COA1 \$129.1M	\$123.5M	\$0	(\$364.9M)	\$119.8 M
COA2 \$493.9M	\$488.3M	\$364.9M	\$0	\$484.6M
COA3 \$9.3M	\$3.7M	(\$119.8M)	(\$484.6 M)	\$0

By comparing the results in Table 12, 13, 14, and 15, one can see that the cost differences between the COAs are slowly changing throughout the years. For example, the cost differences between COA 0 and COA 1 are \$122.2M, \$122.6M, \$123.1M, and \$123.5M, after the first, third, sixth, and ninth year, respectively. A minimal change is observed, thus the costs of the COAs have a similar rate of increase throughout the years.

Since COA 0 is the baseline, the following analysis is with respect to the price of COA 0 and the initial cost of the COAs, with the assumption that all four warfare centers implement the same COA:

- It will take approximately 198 years for COA 2 to break even.
- It will take approximately 788 years for COA 2 to break even.
- It will take approximately three years for COA 3 to break even.

The warfare centers receive a total yearly budget of approximately \$6,000,000 to expand the various LBTS's capability (Defense & Aerospace Competitive Intelligence Service [DACIS] 2019). With this budgetary constraint on implementation, it will take 20 years and 81 years to implement COA 1 and COA 2, respectively. COA 3 will be implemented in one year.

B. RISK ANALYSIS

Risks were analyzed in accordance with the Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (United States Department of Defense [U.S. DOD] 2017). DOD defines risk as a “potential future event or condition that may have a negative effect on achieving program objectives for cost, schedule, and performance” (U.S. DOD 2017).

1. Risk Management Process

The team used the DOD's five-step risk management process shown in Figure 33: Process Planning, Identification, Analysis, Mitigation/Correction, and Monitoring (U.S. DOD 2017). During the risk process planning, the team developed, implemented, and documented steps to mitigate individual risks. To identify potential risks, the team answered questions from U.S. DOD (2017) such as, “What can go wrong? or What is particularly difficult to accomplish?.” U.S. DOD's (2017) risk analysis consisted of answering questions such as, “What is the likelihood that the risk will occur? What are the consequences/impact of the risk? What is the risk level?” The risk mitigation strategy answered questions such as, “What is the plan to address the risk? or Should the risk be accepted, avoided, transferred, or controlled?” (U.S. DOD 2017). The risk monitoring consisted of answering questions such as, “How has the risk changed? or How are the risk mitigation plans working? ... Should additional actions be taken to mitigate or control the risk?” (U.S. DOD 2017).



Figure 33. Risk and Issue Management Process Overview. Source: United States Department of Defense [U.S. DOD] (2017).

2. Risk Identification and Assessment

Risks are defined by their probability of occurrence and their consequences/impact, or severity, as in Figure 34. The risks can affect the cost, schedule, and technical performance of the project. The overall consequence of the risk was determined by the highest consequences level of the cost, schedule, or technical performance. A risk matrix was used to convert the likelihood and consequences of the risks to form a visual display of the risk level of each identified risk, as shown in Figure 34. The risk level of a risk is plotted by using the likelihood level on the x-axis and the consequence level on the y-axis. The risk level of each identified risk is reported as low (green), moderate (yellow), or high (red). The risk matrix facilitates the communication of the severity of the risks.

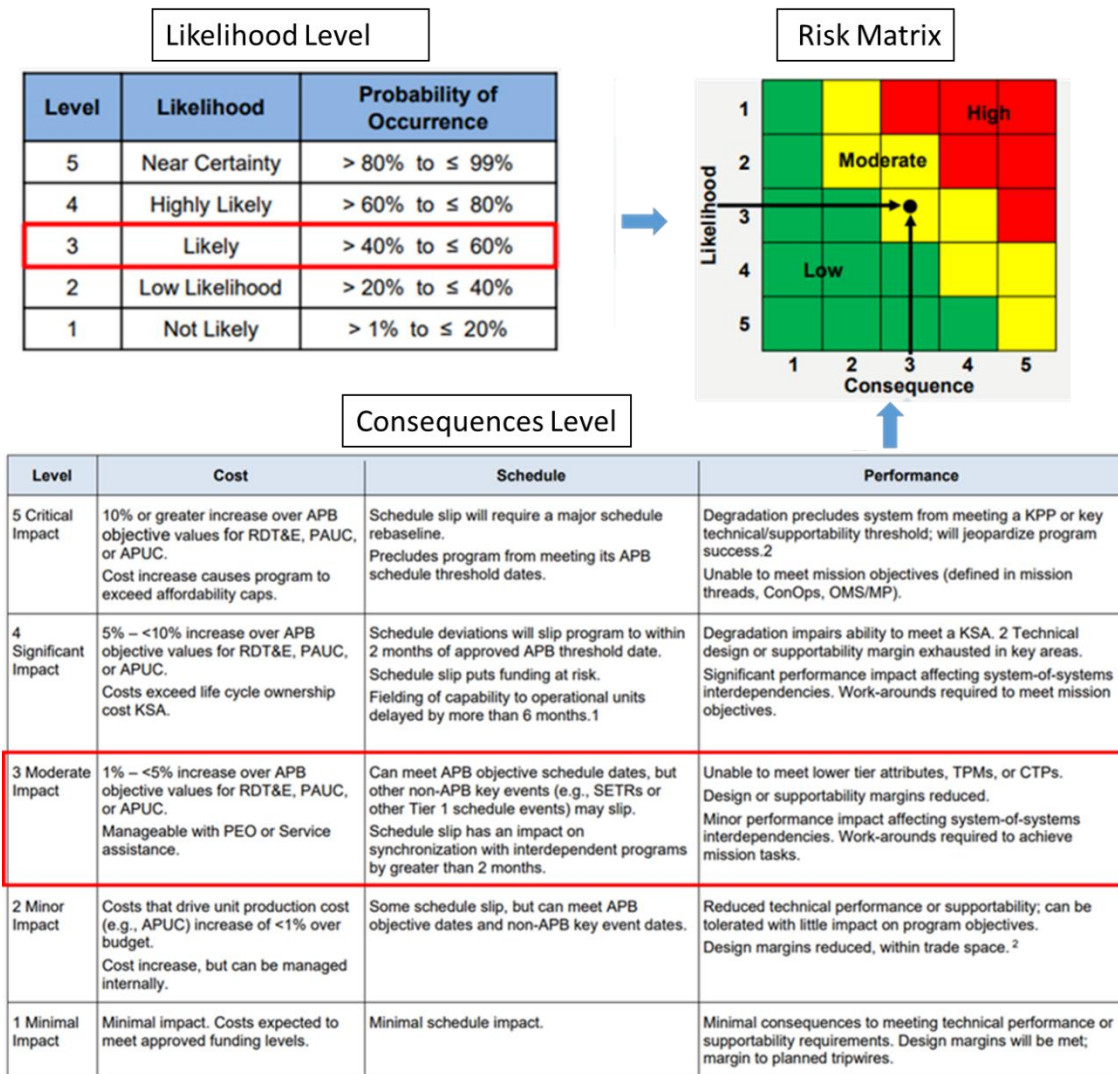


Figure 34. Risk Reporting Matrix and Criteria. Source: United States Department of Defense [U.S. DOD] (2017).

a. COA 0 Risks and Mitigation Strategies

The team identified COA 0's risks discussed next and presented in Table 16. After identifying the risk levels, the team created mitigation strategies to reduce the likelihood of the risks to occur, hence decreasing the risks levels as shown in Table 17.

- **Risk 1, Availability:** If the ships are not available, then the tasks will not be performed.

Mitigation Strategy: Plan accordingly. Create a back-up plan in case the scheduled ship is not available. Constantly verify the schedule of the ships in case of any deviation.

- **Risk 2, Availability:** If the rules and regulations onboard the ship are not met, then the tasks will not be performed.

Mitigation Strategy: Be familiar with all the regulations and comply with them. Obtain access authorization in a timely manner.

- **Risk 3, Accuracy:** If the integrated area is exposed to a harsh environment, then the integrated system can be damaged.

Mitigation Strategy: Carefully determine where the work must be placed. Avoid areas that can easily be damaged or areas that are exposed to harsh environments. Survey the area, when possible, to check if any damage has occurred.

- **Risk 4, Familiarity:** If the systems in the ships are complex or new, then one will not be able to understand the systems and complete the tasks.

Mitigation Strategy: Be familiar with the system prior to completing the work. Be up-to-date and familiar with any upgrade or new technology that can affect performing the tasks.

Table 16. Course of Action (COA) 0 Risk Analysis Before Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Availability	Ship not available	5 Near Certainty	3 Moderate	4 Significant	4 Significant	4 Significant	High
2	Accessibility	Unable to access the ship	3 Likely	3 Moderate	4 Significant	4 Significant	4 Significant	Moderate
3	Accuracy	Damaged work	2 Low Likelihood	4 Significant	4 Significant	4 Significant	4 Significant	Moderate
4	Familiarity	Unable to understand the systems	2 Low Likelihood	3 Moderate	4 Significant	4 Significant	4 Significant	Moderate

Table 17. Course of Action (COA) 0 Risk Analysis After Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Availability	Ship not available	2 Low Likelihood	3 Moderate	4 Significant	4 Significant	4 Significant	Moderate
2	Accessibility	Unable to access the ship	1 Not Likely	3 Moderate	4 Significant	4 Significant	4 Significant	Low
3	Accuracy	Damaged work	1 Not Likely	4 Significant	4 Significant	4 Significant	4 Significant	Low
4	Familiarity	Unable to understand the systems	1 Not Likely	3 Moderate	4 Significant	4 Significant	4 Significant	Low

b. COA 1 Risks and Mitigation Strategies

The team identified the risks of COA 1 discussed next and presented in Table 18. After identifying the risk levels, the team created mitigation strategies to reduce the likelihood of the risks to occur, hence decreasing the risks levels as shown in Table 19.

- **Risk 1, Availability:** If the lab has multiple users, then schedule conflict can cause delays.

Mitigation Strategy: Clearly communicate the schedule to the users. Create a scheduling tool available for use by all users to see when the lab is available and to reserve a time.

- **Risk 2, Availability:** If the lab is down for maintenance or any other reasons, then tasks will not be performed.

Mitigation Strategy: Clearly communicate the schedule with the users. Include Maintenance and other services in the master schedule provided to all the users.

- **Risk 3, Accessibility:** If traveling to the lab is impacted (restrictions like the pandemic or access regulation), then the task will not be performed.

Mitigation Strategy: Plan accordingly. Be familiar with all the regulations and comply with them. Obtain access authorization in a timely manner.

- **Risk 4, Obsolete:** If the facility is not built to accommodate future additions or upgrades, then the lab may be outdated and unable to be used in the future.

Mitigation Strategy: Use forward thinking when designing and building the labs. Anticipate innovation and include a plan for future updates.

Table 18. Course of Action (COA) 1 Risk Analysis Before Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Availability	Delays caused by schedule conflict	5 Near Certainty	3 Moderate	4 Significant	4 Significant	4 Significant	High
2	Availability	Lab being down	5 Near Certainty	3 Moderate	4 Significant	4 Significant	4 Significant	High
3	Accessibility	Unable to travel to the lab	2 Low Likelihood	3 Moderate	4 Significant	4 Significant	4 Significant	Moderate
4	Obsolete	Unable to be upgraded	2 Low Likelihood	2 Minor	2 Minor	4 Significant	4 Significant	Moderate

Table 19. Course of Action (COA) 1 Risk Analysis After Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Availability	Delays caused by schedule conflict	2 Low Likelihood	3 Moderate	4 Significant	4 Significant	4 Significant	Moderate
2	Availability	Lab being down	2 Low Likelihood	3 Moderate	4 Significant	4 Significant	4 Significant	Moderate
3	Accessibility	Unable to travel to the lab	1 Not Likely	3 Moderate	4 Significant	4 Significant	4 Significant	Low
4	Obsolete	Unable to be upgraded	1 Not Likely	2 Minor	2 Minor	4 Significant	4 Significant	Low

c. COA 2 Risks and Mitigation Strategies

The team identified the potential risks of COA 2 discussed next and presented in Table 20. After identifying the risk levels, the team created mitigation strategies to reduce the likelihood of the risks to occur, hence decreasing the risks levels as shown in Table 21.

- **Risk 1, Obsolete:** If the facility is not built to accommodate future additions or upgrades, then the lab may be outdated and unable to be used in the future.

Mitigation Strategy: Use forward thinking when designing and building the labs. Anticipate innovation and include a plan for future updates.

- **Risk 2, Availability:** If the lab is down for maintenance or any other reasons, then tasks will not be performed or travel to a different lab will be necessary.

Mitigation Strategy: Clearly communicate the schedule to the users. Include Maintenance and other services in the master schedule provided to all the users. Plan on completing works when there is less disruption.

Table 20. Course of Action (COA) 2 Risk Analysis Before Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Obsolete	Unable to be upgraded	2 Low Likelihood	2 Minor	2 Minor	4 Significant	4 Significant	Moderate
2	Availability	Lab being down	5 Near Certainty	3 Moderate	4 Significant	4 Significant	4 Significant	High

Table 21. Course of Action (COA) 2 Risk Analysis After Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Obsolete	Unable to be upgraded	1 Not Likely	2 Minor	2 Minor	4 Significant	4 Significant	Low
2	Availability	Lab being down	2 Low Likelihood	3 Moderate	4 Significant	4 Significant	4 Significant	High

d. COA 3 Risks and Mitigation Strategies

The team identified the risks of COA 3 discussed next and presented in Table 22. After identifying the risk levels, the team created mitigation strategies to reduce the likelihood of the risks to occur, hence decreasing the risks levels as shown in Table 23.

- **Risk 1, Vulnerability:** If one of the nodes/systems is compromised by a cyberattack, then the security threats can propagate to other nodes/systems through the interconnected gateways.

Mitigation Strategy: Minimize the attack surfaces, like firewalls and software updates, by monitoring all the vulnerabilities. Segregate the different subsystems and use defense strategies to block unwanted traffic.

- **Risk 2, Confidentiality:** If the end-to-end communication is not secured, then information can be disclosed to unauthorized personnel.

Mitigation Strategy: Since the risk level is low, it can be accepted and monitored. The following plan can be utilized if further actions are required: Use the zero-trust network access—never trust, always verify. Limit and control access to the network. Identify credentials, authorization, and the need to know prior to granting access to the system.

- **Risk 3, Availability:** If the system is down because of an unintentional event (such as software failure or operator error), then all the functionality of the system will be interrupted.

Mitigation Strategy: Communicate cybersecurity policies and procedure (specialized trainings) well and often to reduce the likelihood of unintentional threats. Perform preventive maintenance routinely to reduce premature failure. Incorporate redundant assets in critical areas to provide a backup in case of failure.

- **Risk 4, Availability:** If the system is down because of intentional event (cyberattack, sabotage, and the like), then all the functionality of the system will be interrupted.

Mitigation Strategy: Always assume that an attack has occurred and take proactive measures to identify, contain and remove the threat. Use automated tools to identify potential threats before they occur. Utilize multifactor authentication to prevent unauthorized access.

- **Risk 5, Integrity/Reliability:** If the transmitted data is compromised, not accurate and/or not complete, then the system will be unreliable.

Mitigation Strategy: Utilize a Network Operations Center that monitors data traffic health status.

Table 22. Course of Action (COA) 3 Risk Analysis Before Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Vulnerability	Propagation of security threats	2 Low Likelihood	3 Moderate	3 Moderate	4 Significant	4 Significant	Moderate
2	Confidentiality	Unauthorized disclosure	2 Low Likelihood	2 Minor	2 Minor	3 Moderate	3 Moderate	Low
3	Availability	System being down (unintentional)	3 Likely	2 Minor	4 Significant	4 Significant	4 Significant	Moderate
4	Availability	System being down (intentional)	2 Low Likelihood	2 Minor	4 Significant	4 Significant	4 Significant	Moderate
5	Integrity/Reliability	Transmitting compromised or inaccurate data	2 Low Likelihood	2 Minor	2 Minor	4 Significant	4 Significant	Moderate

Table 23. Course of Action (COA) 3 Risk Analysis After Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Vulnerability	Propagation of security threats	1 Not Likely	3 Moderate	3 Moderate	4 Significant	4 Significant	Low
2	Confidentiality	Unauthorized disclosure	1 Not Likely	2 Minor	2 Minor	3 Moderate	3 Moderate	Low
3	Availability	System being down (unintentional)	1 Not Likely	2 Minor	4 Significant	4 Significant	4 Significant	Low
4	Availability	System being down (intentional)	1 Not Likely	2 Minor	4 Significant	4 Significant	4 Significant	Low
5	Integrity/Reliability	Transmitting compromised or inaccurate data	1 Not Likely	2 Minor	2 Minor	4 Significant	4 Significant	Low

Each COAs have their set of risks that must be considered when implementing them. COA 0 and COA 1 have the highest risk associated with the availability of the ship or the lab, respectively, which could be lowered to a moderate level utilizing the identified mitigation plan. The rest of the COAs have low to moderate risks that could be lowered by implementing their mitigation plan.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. ANALYSIS SUMMARY

The objective of this capstone is to examine alternative means by which PHD and other NSWCs can collaborate more effectively to provide a better and more cost-effective product for the naval fleet. Technical feasibility, earned value to the organization, time for implementation, schedule risk, and other risk are all critical aspects to the success of a COA. Each COA's combined index indicates the weighted success of all five components.

Technical feasibility is the probability that a product or service can be successfully implemented with current technology. COA 1 and COA 2 have the same architectural design as COA 0, and thus it is assumed that the technical feasibility would reflect that of COA 0, that being 100%. COA 3's technical feasibility will be based on the throughput of successful packages flowing from lab to lab. As this value is largely dependent on the distance between the labs, the team considered the distance from PHD to Dahlgren for this report. PARM should consider the varied distances between the different connecting labs when utilizing this framework.

An evaluation of EV is based on the number of use cases the system can complete. The use cases (UC) that can be accomplished by each COA are shown in Table 24 where an "X" indicates a uses case is accomplished successfully by a specific COA. An EV index is assigned to the COAs based on the proportion of achievable use cases to the proportion of required use cases.

Table 24. Evaluation of the Earned Value

Use Cases	COA 0	COA 1	COA 2	COA 3
UC-1 Fleet Support	X	X	X	X
UC-2.1 IV &V	X	X	X	X
Four UC-2.2 System Integration Test	X	X		X
UC-2.3 Operational Kill-Chain Test	X	X	X	

Use Cases	COA 0	COA 1	COA 2	COA 3
UC-3.1 Maintenance Requirement Cards	X	X	X	X
UC-3.2 Software Installation Procedures	X	X	X	X
UC-3.3 Standard Operating Procedures	X	X	X	X
UC – 3.4 Technical Manuals	X	X	X	X
UC – 4.1 Hardware Development		X	X	X
UC – 4.2 Software Development	X	X	X	X
UC – 5.1 Interoperability Training	X	X	X	
UC -5.2 Emulator Training	X	X	X	X
Earned Value Index	92%	100%	100%	83%

A cost analysis was performed to estimate the cost of the various COAs using DOD past budgets for LBTS, past budgets for testing environments, and the current costs to perform the use cases. COA 0 has a recurring cost from TDY, which is estimated to cost \$155,000 per year for each warfare center, and \$620,000 per year for four warfare centers. COA 1 has an initial cost of \$122,211,200 for the set-up of one fully integrated lab and obtaining an initial ATO, a recurring cost of \$422,400 every three years for maintaining the ATO, and a recurring TDY cost of \$155,000 per year for each participating warfare center. COA 2 has an initial cost of \$488,844,800 for the set-up of four fully integrated labs for the four warfare centers and obtaining initial ATOs, in addition of a recurring cost of \$1,689,600 every three years for maintaining the ATOs. Since most of the networks that COA 3 could use incur no network operations and equipment costs as they are covered by an external agency, COA 3 has an initial cost of \$1,689,600 for the initial cost of the ATOs and \$2,534,400 every three years for maintaining the ATOs in four warfare centers. If all the four warfare centers implement the same COA, by using the price of COA 0 as a baseline and the initial cost of the COAs, the team determined that it would take 198 years for COA 1 to break even, 788 years for COA 2 to break even, and three years for COA 3

to break even. With the current yearly budget constraint of \$6,000,000 that the warfare centers receive to expand the LBTS, COA 3 will be implemented in one year. However, it will take 20 years, and 81 years to implement COA 1 and COA 2, respectively. As a combat system is assumed to have a five-year lifespan before requiring modernization, any COA with an implementation time exceeding five years is assumed to have failed to meet the requirements as it is outdated and no longer representative of a shipboard system. Additionally, any COAs with break-even dates more than a few decades into the future have significant uncertainty in the true final break-even date. Thus, while COA break-even times above five years are provided in this paragraph, any COA with a break-even of longer than five years can be discounted.

A risk analysis was also completed, during which the team identified the risks of each COA and provided mitigation strategies for them. Each COAs has its set of risks that must be considered when utilizing them. COA 0 and COA 1 highest risk are associated with the availability of the ship or the lab, respectively, which could be lowered to a moderate level by utilizing the identified mitigation plans, such as planning accordingly, constantly verifying the schedule of the ship or the lab, and clearly communicating the schedule with the users. COA 2 and COA 3 have low to moderate risks that could be lowered by implementing the proposed mitigation plans.

The COAs were evaluated with respect to the identified evaluation measures: Time to implement, earned value, technical feasibility, scheduling risk, and other risks, as shown in Table 25. The evaluation measures were chosen based on the stakeholders' needs and the system requirements. A relative weight was assigned to each evaluation measure based on presumed importance to the stakeholders. Then, each COA was given a score between 1 to 10 (one being worst and ten being the best) based on how well they satisfy the evaluation measures. During the cost analysis, the duration it takes to implement each COAs was calculated, and the results were utilized when scoring the COAs. The identified risks and mitigation strategies evaluated during the risk analysis were also considered when scoring the COAs on the scheduled risk (availability of the lab or ship) and the other risks. During the analysis of the various COAs, the team evaluated and scored the EV and the technical feasibility of each COAs. The total scores were obtained by summing the product

of the weights and the corresponding score for each COA. The team considered the scores of the solutions alternative to the current state of operations, COA 0, and observed that COA 3 has the highest score while COA 2 has the lowest score. The matrix results can be interpreted as the higher the total score, the better the alternative, thus COA 3 is interpreted to be the best COA.

Table 25. Weighted Evaluation Matrix of the Courses of Action (COAs)

	Time to Implement	Earned Value	Technical Feasibility	Scheduling Risk	Other Risks	Total Score
Weight	2	3	3	1	1	
COA 0 (Current Set-up)	10	9	10	5	7	89
COA 1 (One Integrated Lab)	4	10	10	6	6	80
COA 2 (Multiple Integrated Labs)	1	10	10	10	6	78
COA 3 (NOLIN)	9	8	8	9	8	83

To summarize, all evaluated COAs meet the requirements to perform most of the required use cases, as described in Table 25. The team recommends the implementation of COA 0 as an alternative to COA 1–3. Based on an evaluation of the COAs in terms of their benefits and costs, COA 0 provides more value. A visual representation of this conclusion can be found in Figures 35 and 36. Figure 35 presents the COAs with respect to their benefits and costs. As a result of using the cost analysis process, it is evident that COA 0 provides the most “bang for the buck.” This can be attributed due to the lower reoccurring cost associated with COA 0 vice COA 3. Figure 36 illustrates this further, with COA 0 having a significantly greater cost-benefit ratio.

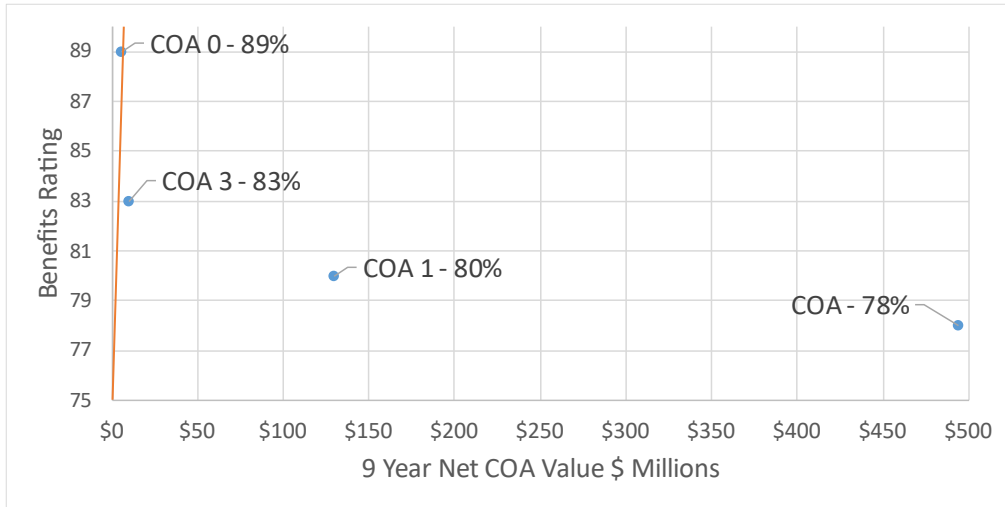


Figure 35. Cost vs. Benefits of the COAs

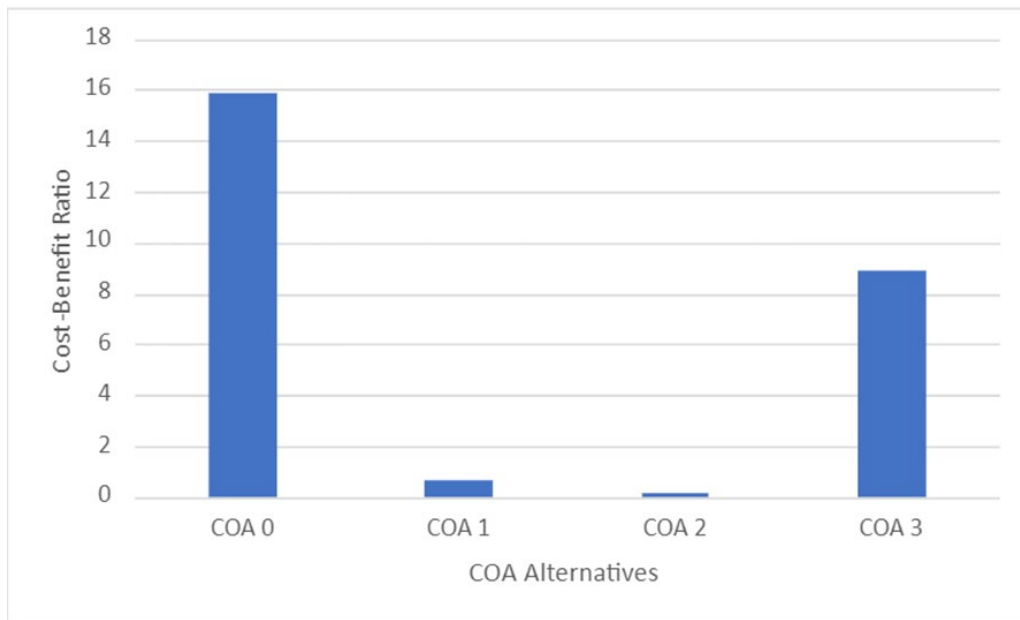


Figure 36. Cost- Benefit Ratio of the COAs

THIS PAGE INTENTIONALLY LEFT BLANK

X. CONCLUSION

NAVSEA warfare centers are serving as LBTs for testing and certifying weapon systems prior to delivery to the Fleet. However, the LBTs are distributed geographically across the United States and lack the representation of a fully integrated combat system. As a result, ships are used to perform the testing, which takes a significant amount of planning and travel costs. This capstone report was developed to analyze the approaches of creating a unified capability LBT able to connect the separate and independent labs and enable collaboration and testing using a fully integrated platform.

By applying the SE process, the NPS MSSE One Navy Lab team evaluated a variety of COAs with the goal of providing the Navy Fleet with the most efficient solutions. Four COAs were identified based on the stakeholders' needs. COA 0 is to keep the current set-up and the engineers will continue to travel to existing LBTs and ships for testing. COA 1 is to build one fully integrated combat systems lab that will be shared among the different warfare centers. For COA 2, each warfare center will have a fully integrated combat system. COA 3 connects separate and independent labs using a DOD network.

As part of this comprehensive analysis, the alternative COAs were carefully compared, taking into account their respective advantages and disadvantages against critical criteria. During the process, a cost analysis was performed to estimate the cost of the various COAs. A risk analysis was also conducted to identify the potential risks of the COAs and their mitigation plans. As a result of the team's discernment, COA 0 was chosen, emphasizing the status quo as the most advantageous option when compared to the alternatives such as the integration of a network into existing labs or building new LBTs. A structured methodology is offered by this report to enable program managers to make well-informed decisions for future implementations.

A. FUTURE WORK

The following sections explore possibilities for future research to refine and expand on the team's current findings, including additional simulations and testing within DOD network, development of lab-specific software, and exploration of virtualized systems.

1. Additional testing within the DOD network

It is important to develop a simulation model based on the specific DOD network in order to ensure an accurate simulation. This includes incorporating more information from the network itself, currently unavailable to this report due to non-Distribution A classification levels, such as hardware lists, network security configurations, and other factors that affect the key performance parameters in the simulation. Implementing the network parameters will provide a simulation that better represents the actual network. Thus, a much more accurate idea of the network's actual performance within the real environment can be obtained. In addition to network simulations, a thorough understanding of system specific network requirements for each use-case should be evaluated and compared to the simulation results.

During the verification and validation process, network testing should be done to identify any potential issues before proceeding with implementation. Network testing should be conducted before, during, and after implementation to ensure that it is working correctly.

2. Lab Software Configuration

There is also a possibility that the software configuration needs to be changed. The current kernel configuration specifies the latency requirements for packets based on the system's function. It could be possible to accomplish hard real-time application use-cases with lab-specific software that is designed to accommodate WAN tolerant latency requirements.

3. Virtualized System Analysis

There is also the possibility of utilizing virtual systems as a COA. Virtualized systems have become increasingly popular within the defense community since they provide a cost-effective alternative to software-related testing. Nevertheless, a virtual system is only as good as the fidelity of the machine. The analysis for implementation of virtual systems, COA 4, has been developed in appendix C. A future step for COA 4 will be to conduct the feasibility study based on the specific use-case application requirements.

APPENDIX A: EXTENDSIM MODELING EMPIRIC TABLES AND CODE

EMPIRIC TABLES AND CODE

Table 26. ISP Probability of Packet Failure Empiric

Packet Success	Probability
GO	87.1%
NO-GO	12.9%

Table 27. ISP Jitter Probability Empiric

Jitter Delay ms	Probability
0	0.2%
1	6.8%
2	27.1%
3	20.6%
4	8.5%
5	6.8%
6	4.8%
7	4.0%
8	2.2%
9	1.4%
10	1.2%
11	0.6%
12	0.8%
13	1.6%
14	1.1%
15	0.7%
16	0.5%
17	0.6%
18	0.5%
19	0.2%
20	0.1%
21	0.4%
22	0.2%
23	0.5%

24	0.4%
25	0.3%
26	0.2%
27	0.3%
28	0.1%
29	0.2%
31	0.3%
32	0.3%
33	0.1%
34	0.2%
35	0.2%
36	0.2%
37	0.1%
41	0.1%
42	0.1%
43	0.2%
44	0.1%
45	0.1%
47	0.1%
49	0.1%
50	0.1%
52	0.1%
53	0.1%
54	0.1%
55	0.1%
56	0.1%
58	0.1%
60	0.1%
62	0.1%
63	0.1%
64	0.1%
65	0.1%
67	0.1%
70	0.1%
72	0.1%
74	0.1%
75	0.1%
78	0.1%
80	0.1%
81	0.1%

82	0.1%
83	0.1%
84	0.1%
85	0.1%
90	0.2%
91	0.1%
92	0.1%
93	0.1%
94	0.2%
100	0.2%
101	0.1%
102	0.1%
103	0.1%
104	0.2%
105	0.1%
110	0.1%
111	0.1%
112	0.2%
114	0.2%
115	0.1%
116	0.1%
118	0.1%
120	0.1%
122	0.1%
123	0.1%
124	0.1%
125	0.1%
130	0.1%
131	0.1%
132	0.1%
134	0.1%
135	0.1%
136	0.1%
140	0.1%
142	0.1%
144	0.1%
145	0.1%
147	0.1%
149	0.1%
152	0.1%

153	0.1%
155	0.1%
157	0.1%
159	0.1%
161	0.1%
162	0.1%
165	0.1%
167	0.1%
169	0.1%
171	0.1%
172	0.1%
175	0.1%
177	0.1%
179	0.1%
180	0.1%
185	0.1%
186	0.1%
191	0.1%
195	0.1%
196	0.1%
205	0.1%
217	0.1%
227	0.1%
237	0.1%
247	0.1%
257	0.1%

ExtendSim Code:

```
//*****
//START: Equation Variables – Block 77

//Input Variables
//-----
//    1.) inDistance (Type = Connector 0)
//    2.) inPacketSize (Type = Connector 1)
//    3.) inFireCrypLat (Type = Connector 2)
//    4.) inProtocol (Type = Connector 3)
//    5.) inJitterDelay (Type = Connector 4)
```

```

//    6.) inQueue (Type = Connector 5)
//    7.) inHistTotalLat (Type = Connector 6)

//Output Variables
//-----
//    1.) outDelay (Type = Connector 0)
//    2.) outTotalLatency (Type = Connector 1)

//END: Equation Variables
//*****
double Distance;
double PacketSize;
double FireCrypLat;
double Protocol;
double JitterLat;

double CopperPath;
double FiberPath;
double Transponder;

double PropagationDelay;
double TransmissionDelay;
double SerializationDelay;
double QueueDelay;
double TotalLatency;

double RTT;
double RTTtout;
double TCPACK;

Distance = inDistance;
PacketSize = inPacketSize;
Protocol = inProtocol;

// Firewall and Encryption Calculation
FireCrypLat = inFireCrypLat;

//Jitter Delay Calculation
JitterLat = inJitterDelay;

```

```

//D Queue Delay
QueueDelay = inQueue;

//D propagation Calculation
CopperPath = (Distance * 0.05)/(299.792*0.65); //Distance Has to be in Km
FiberPath = ((Distance * 0.95)/299.792)*1.4711; //Distance Has to be in Km
Transponder = (((Distance*0.95)/5)*0.005); //Assuming that the copper section is
retransmission is negligible
PropagationDelay = CopperPath + FiberPath + Transponder;

//D serialization Calculation
SerializationDelay = 0.001;
//D Transmission Calculation Assume 35.13 Mbps converted to 4391.25 bytes per
millisecond
TransmissionDelay = PacketSize/4391.25;

// Round Trip Calculation
RTT = PropagationDelay+SerializationDelay+JitterLat+TransmissionDelay;

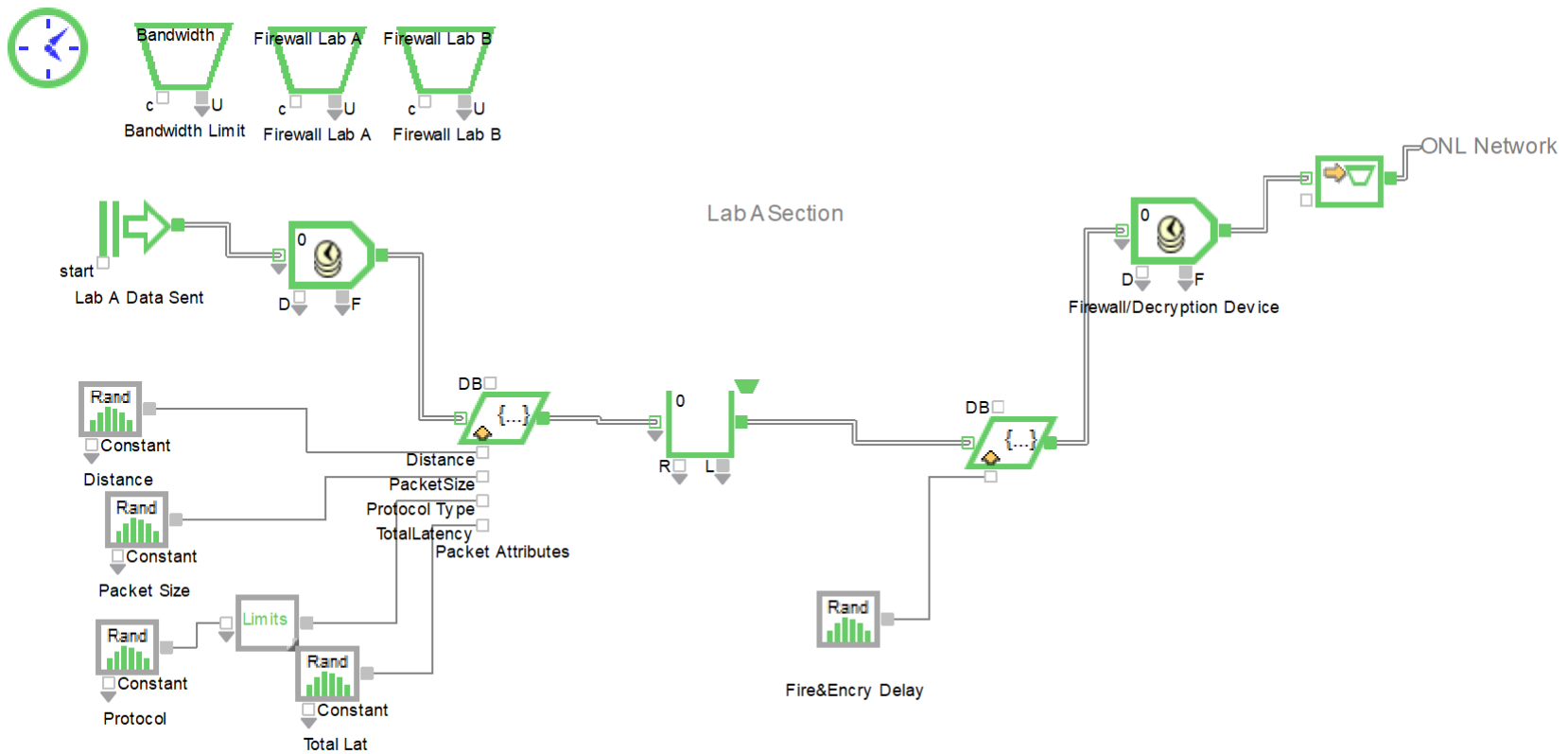

// Protocol Based RTT Output
IF(Protocol < 1)
    RTTOut = RTT*1;

ELSE
    TransmissionDelay = 43/4391.25;
    TCPACK = PropagationDelay+SerializationDelay+JitterLat+TransmissionDelay;
    RTTOut = RTT+TCPACK;

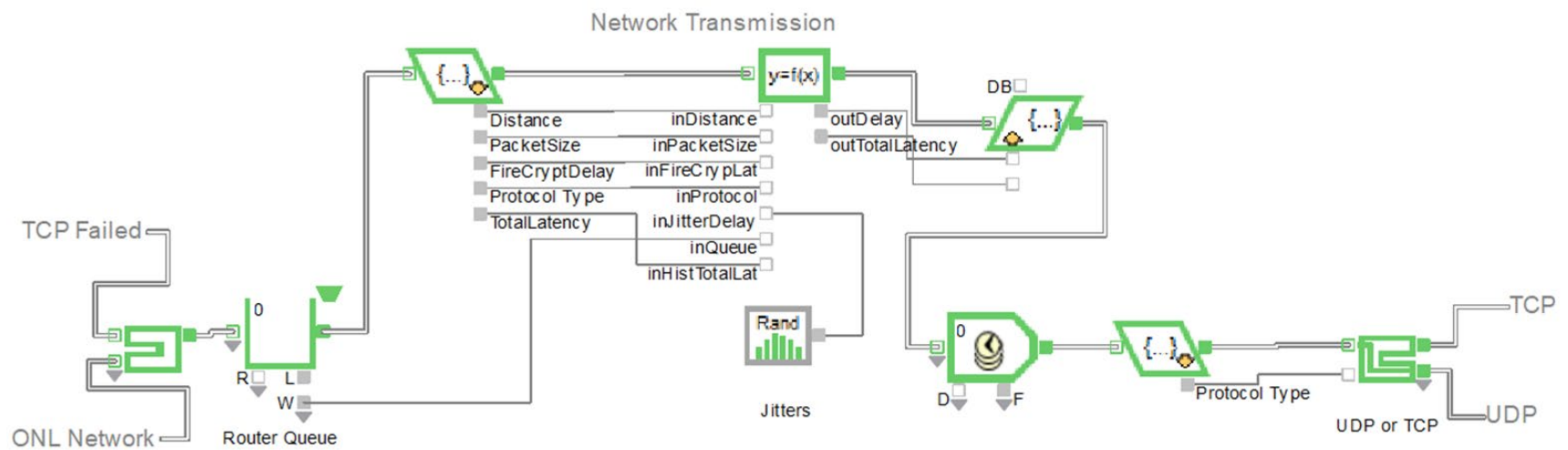
outDelay = RTTOut;
outTotalLatency = inHistTotalLat + RTTOut + FireCrypLat + QueueDelay;

```

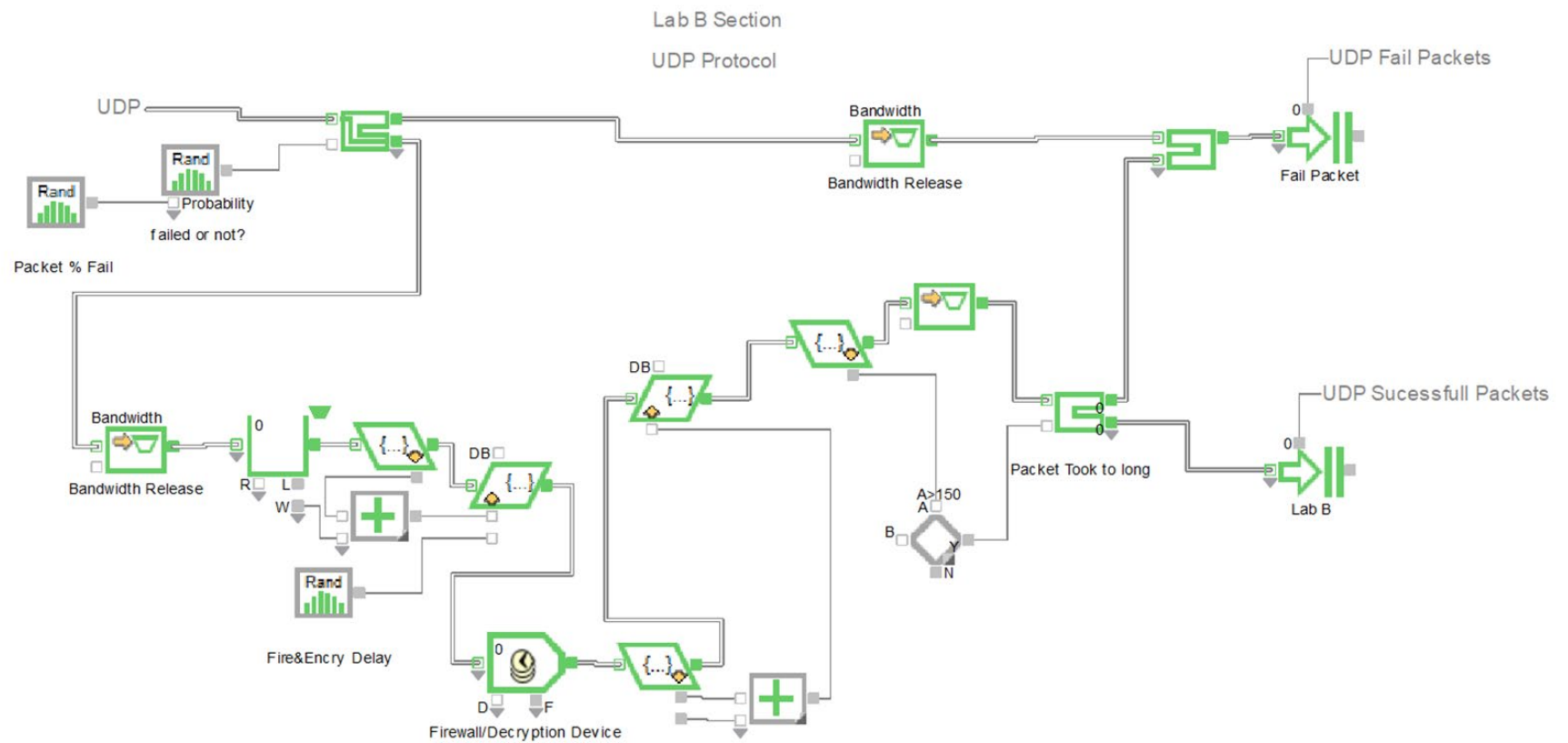
PACKET ORIGINATOR SECTION MODEL



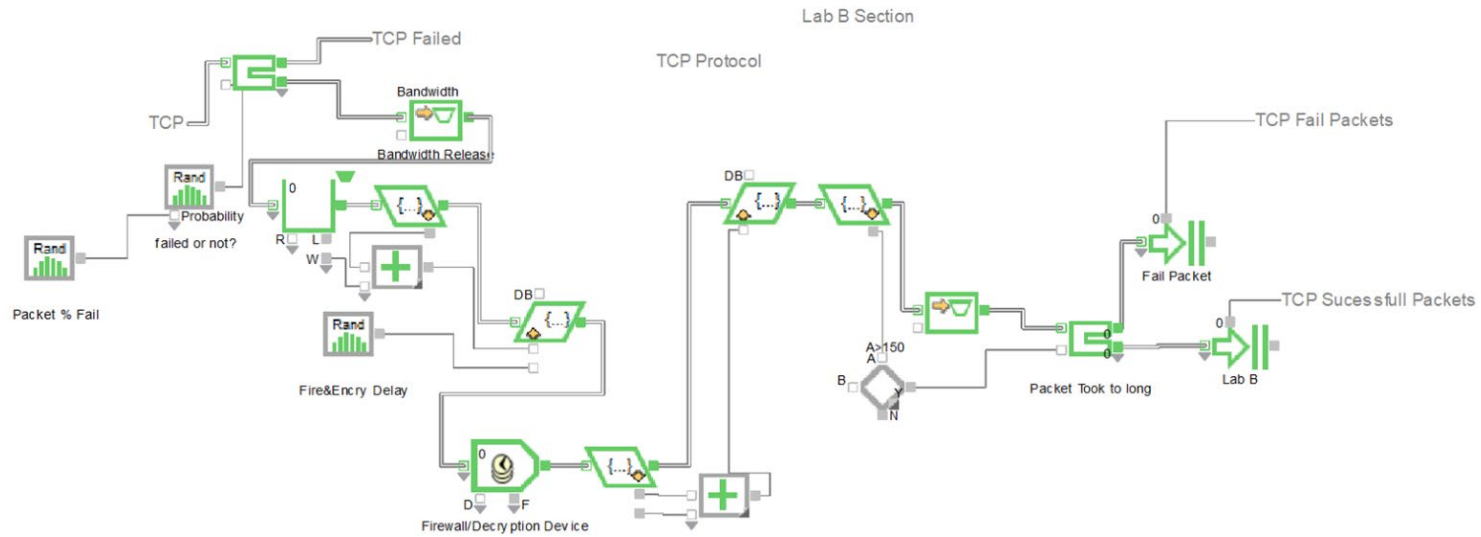
NETWORK TRANSMISSION SECTION MODEL



PACKET RECEIVER FOR UDP MODEL



PACKET RECEIVER FOR TCP MODEL



APPENDIX B: COST ANALYSIS ASSUMPTIONS

The following assumptions were made when completing the cost analysis:

- Four warfare centers are part of the One Navy Lab.
- Each warfare center completes eight temporary duties (TDY) per year.
- Each TDY takes four weeks to complete.
- Two personnel participated in each TDY.
- The labor rate is \$220 per hour.

The following assumptions were made when calculating the cost of TDY from PHD to Norfolk, VA:

- Two GS12 personnel per travel
- Number of travels: Two per quarter, eight per year
- Duration of each travel: Four weeks
- Hourly wage: \$220
- Comp time per Trip: 15 hours ~ \$3300
- Flight Cost: \$800
- Car rental and fuel Cost: \$2000
- Lodging Cost: \$2000
- Per diem: \$1300

The following assumptions were made when calculating the cost of TDY from PHD to Hawaii:

- Two GS12 personnel per travel

- Number of travels: Two per quarter, eight per year
- Duration of each travel: Four weeks
- Hourly wage: \$220
- Comp time per Trip: 17 hours ~ \$3740
- Flight Cost: \$1050
- Car rental and fuel Cost: \$1400
- Lodging Cost: \$3100
- Per diem: \$3375

The following assumptions were made when calculating the cost of TDY from PHD to San Diego:

- Two GS12 personnel per travel
- Number of travels: Two per quarter, eight per year
- Duration of each travel: Four weeks
- Hourly wage: \$220
- Comp time per Trip: 2 hours ~ \$440
- Flight Cost: \$300
- Car rental and fuel Cost: \$1100
- Lodging Cost: \$4074
- Per diem: \$1590

The following assumptions were made when calculating the cost of TDY from PHD to Indian Head:

- Two GS12 personnel per travel
- Number of travels: Two per quarter, eight per year
- Duration of each travel: Four weeks
- Hourly wage: \$220
- Comp time per Trip: 10 hours ~ \$2200
- Flight Cost: \$800
- Car rental and fuel Cost: \$2800
- Lodging Cost: \$2000
- Per diem: \$1268

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: COURSE OF ACTION (COA) 4

COA 4: INTEGRATION OF VIRTUALIZED SYSTEMS

The team identified integration of virtualized naval elemental systems with non-virtualized naval elemental systems to create a fully integrated combat systems lab. This configuration, as seen in Figure 37, is the fourth COA proposed as a potential alternative One Navy Lab solution. The virtualized systems are desktop computer set-ups that emulate the elemental system it represents. Live data for the virtualized element—such as radar data—will be recorded and downloaded from a real radar system from elsewhere—another lab or a ship—and will be sent to the lab housing the virtualized system via shipment or a file-sharing network. This data will then be uploaded to the virtualized system and be used like the real element’s data, e.g., radar data will be uploaded to the virtualized radar system and the virtualized radar system will send over that target radar data to the CMS for the CMS to track the target and engage a weapon system to it. Using these systems, the operations of a variety of baselines can be replicated. COA 4 would require procurement of equipment required for the virtualized systems the respective NSWC requires and the associated cybersecurity costs.

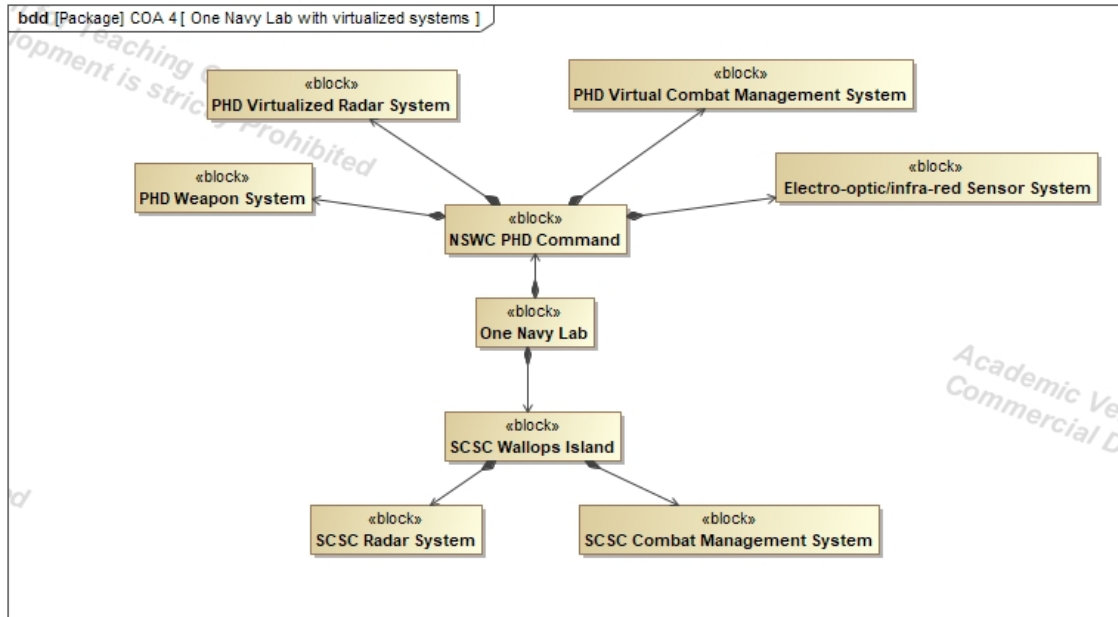


Figure 37. Course of Action (COA) 4 Architecture

COA 4: COST

COA 4 has non-recurring costs associated with acquiring virtualized labs and meeting cybersecurity requirements. In 2009, the Air Force Weather Agency installed a virtualized system that cost \$72,000 (Defense Industry Daily Staff 2011). The equipment for a virtualized testing environment for a Radar costs roughly \$750,000 (NSWC Dahlgren Division Corporate Communications 2021). Since PHD also needs to install a virtualized radar lab, it is assumed a similar cost will be required. Therefore, it is estimated that a non-recurring cost of approximately \$750,000 is required for procuring one virtual equipment set for the One Navy Lab. Since the virtualized labs are considered Zone D, getting an initial ATO is estimated to cost approximately \$211,200 for each lab. With PHD adding two virtualized labs, the cost of implementing the virtualized labs is estimated to be around \$1,500,000 for acquiring them and \$422,400 for the initial ATO request. Additionally, a reauthorization needs to be obtained every three years at the same cost of \$422,400. Moreover, the RMF requires continuous monitoring of the system, which is estimated to cost \$105,600 for each year that reauthorization is not required. Therefore, the cost of maintaining the ATO can be estimated at \$633,600 for every three years. As a result, COA

4 has an initial cost of \$1,922,400 and a recurring cost of \$633,600 for every three years for one warfare center. For four warfare centers, the cost of COA 4 is estimated at an initial cost of \$7,689,600.00, and a recurring cost of \$2,534,400 every three years for maintaining the ATO. With the initial cost, it will take approximately two years for COA 4 to be implemented and about 12 years to break even.

COA 4: RISK AND MITIGATION STRATEGIES

The team identified the risks of COA 4 discussed next and presented in Table 28. After identifying the risk levels, the team created mitigation strategies to reduce the likelihood of the risks to occur, hence decreasing the risks levels as shown in Table 29.

- **Risk 1, Confidentiality:** If the end-to-end communication is not secured, then information can be disclosed to unauthorized personnel.

Mitigation Strategy: Since the risk level is low, it can be accepted and monitored. The following plan can be utilized if further actions are required: Use the zero-trust network access: never trust, always verify. Limit and control access to the network. Identify credentials, authorization and the need to know prior to granting access to the system.

- **Risk 2, Availability:** If the virtualized system is down because of unintentional event (such as software failure or operator error), then all the functionality of the system will be interrupted.

Mitigation Strategy: Communicate cybersecurity policies and procedure (specialized trainings) well and often to reduce the likelihood of unintentional threats. Perform preventive maintenance routinely to reduce premature failure. Incorporate redundant assets in critical areas to provide a backup in case of failure.

- **Risk 3, Availability:** If the virtualized system is down because of an attack on the virtualized system (Jailbreaking, denial-of-service), then all the functionality of the system will be interrupted.

Mitigation Strategy: When appropriate, separate the virtualized machines from the rest of the systems. Use encryption when migrating data. Always assume that an attack has occurred and take proactive measures to identify, contain and remove the threat. Use automated tools to identify potential threats before they occur. Utilize multifactor authentication to prevent unauthorized access.

- **Risk 4, Integrity/Reliability:** If the transmitted data is compromised, not accurate and/or not complete, then the system will be unreliable.

Mitigation Strategy: Utilize a Network Operations Center that monitors data traffic health status.

- **Risk 5, Delay:** If there is a delay in receiving the information, then the timing of critical processes will be affected.

Mitigation Strategy: Program the system to receive real-time data and automatically update information when received.

Table 28. Course Of Action (COA) 4 Risk Analysis Before Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Confidentiality	Unauthorized disclosure	2 Low Likelihood	2 Minor	2 Minor	3 Moderate	3 Moderate	Low
2	Availability	System being down (unintentional)	3 Likely	2 Minor	4 Significant	4 Significant	4 Significant	Moderate
3	Availability	System being down (intentional)	2 Low Likelihood	2 Minor	4 Significant	4 Significant	4 Significant	Moderate
4	Integrity/Reliability	Transmitting compromised or inaccurate data	2 Low Likelihood	2 Minor	2 Minor	4 Significant	4 Significant	Moderate
5	Delay	Delay receiving real-time data	3 Likely	2 Minor	3 Moderate	4 Significant	4 Significant	Moderate

Table 29. Course Of Action (COA) 4 Risk Analysis After Mitigation

Risk #	Topic/Title	Description	Likelihood	Consequence				Overall Risk Level
				Cost	Schedule	Technical	Overall	
1	Confidentiality	Unauthorized disclosure	1 Not Likely	2 Minor	2 Minor	3 Moderate	3 Moderate	Low
2	Availability	System being down (unintentional)	1 Not Likely	2 Minor	4 Significant	4 Significant	4 Significant	Low
3	Availability	System being down (intentional)	1 Not Likely	2 Minor	4 Significant	4 Significant	4 Significant	Low
4	Integrity/Reliability	Transmitting compromised or inaccurate data	1 Not Likely	2 Minor	2 Minor	4 Significant	4 Significant	Low
5	Delay	Delay receiving real-time data	2 Low Likelihood	2 Minor	3 Moderate	4 Significant	4 Significant	Moderate

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Acharya, Anurag and Joel Saltz. n.d. *A Study of Internet Round-Trip Delay*.
<https://api.drum.lib.umd.edu/server/api/core/bitstreams/5cad28a5-4926-40cb-8e11-cbbacad4c8d0/content>.
- AdHoc. n.d. “Authorization to Operate Field Guide.” Accessed October 17, 2023.
<https://adhoc.team/ato/>.
- Akdemir, Kahraman, Martin Dixon, Wajdi Feghali, Patrick Fay, Vinodh Gopal, Jim Guilford, Erdinc Ozturk, Gill Wolrich, and Ronen Zohar. 2010. *White Paper Breakthrough AES Performance with Intel® AES New Instructions*.
<https://www.semanticscholar.org/paper/Breakthrough-AES-Performance-with-Intel-%C2%AE-AES-New-Akdemir-Dixon/62116fe84e7360202d4e1cff859c8fc014ef4614>.
- Angrisani, Leopoldo, and Claudio Narduzzi. 2008. “Testing Communication and Computer Networks: An Overview.” *IEEE Instrumentation & Measurement Magazine*, 11 (5) (October): pp. 12–24. <https://doi.org/10.1109/MIM.2008.4630738>.
- Bah, Mhadi, Prescott Chartier, Jonathan Fraser, Michael Logan, and Isaac Veale. 2018. “Designing an Architecture for a Surface Warfare Mission Module to Be Used by the Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV) in a Chokepoint Scenario.” Systems Engineering Capstone Proposal, Naval Postgraduate School.
- Ball, Latasha. 2021. “Naval Surface Warfare Center, Port Hueneme Division Implements Navy Continuous Training Environment Tool for Live Virtual Constructive Training with the Fleet.” Naval Sea System Command. October 28, 2021.
<https://www.navsea.navy.mil/Media/News/Article/2825743/naval-surface-warfare-center-port-hueneme-division-implements-navy-continuous-t/>.
- Banka, Tarun, Aditya Maroo, Anura. P. Jayasumana, V. Chandrasekar, Nitin Bharadwaj, and SathisKumar Chittibabu. 2005. “Radar Networking: Considerations for Data Transfer Protocols and Network Characteristics.” National Digital Library of India.
- BasuMallick, Chiradeep. 2022. “TCP vs. UDP: Understanding 10 Key Differences.” Spiceworks. April 18, 2022. <https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/>.

- Bay, Morten. 2016. "What is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era." *French Journal For Media Research* (June): 1–28. https://frenchjournalformediaresearch.com/lodel-1.0/main/docannexe/file/988/morten_pdf.pdf.
- Bennett, Caitlin. 2022. "Understanding Stakeholder Needs and Expectations with Data." Consultation Manager. October 18, 2022. <https://www.consultationmanager.com/understanding-stakeholder-needs-and-expectations-with-data/>.
- Carr, J.J., S. L. Saikkonen, and D.H. Williams. 1990. "Refractive Index Measurements on Single-Mode Fiber as Functions of Product Parameters, Tensile Stress, and Temperature." *Fiber and Integrated Optics* 9 (4) (December). <https://doi.org/10.1080/01468039008202927>.
- Carter, Daniel W., Cedric T. Chiu, Timothy O. Hillman, Roianthony Navarro, Harsh Shah, and Victoria Tsugawa. 2020. "Common Combat Systems Remote Software Deployment of Incremental Capability and Updates." Systems Engineering Capstone Report, Naval Postgraduate School. <https://hdl.handle.net/10945/66602>.
- Cisco. 2023. "Cisco Secure Firewall 4100 Series." Cisco. <https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.pdf>.
- Clawson, David A., Sara E. Wallace, Gregory D. Little, and Keith Wheeler. n.d. "Warfare Capability Baseline: Assessing Operational Gaps." NAVSEA. <https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Dahlgren/Resources/Leading-Edge/I-I-Leading-Edge/Clawson/>.
- Coffey, Joseph. 2017. *Latency in Optical Fiber Systems*. WP-111432-EN. CommScope. <https://www.commscope.com/globalassets/digizuite/2799-latency-in-optical-fiber-systems-wp-111432-en.pdf?r=1>.
- Commander, Navy Region Mid-Atlantic. n.d. "Naval Station Norfolk." Accessed November 17, 2023. <https://cnrma.cnmc.navy.mil/Installations/NAVSTA-Norfolk/>.
- The Computing Technology Industry Association (CompTIA). n.d. "What is a Network protocol, and How Does It Work?" Accessed October 19, 2023. <https://www.comptia.org/content/guides/what-is-a-network-protocol>.
- Cordeiro, Raúl and José Manuel Fonseca. 2010. "Euronet Lab: Euronet LAB, a Cloud V-lab Environment." In *5th Iberian Conference on Information Systems and Technologies*. ISBN: 978–989-96247-3-3.
- Dahmouni, Hamza, André Girard, and Brunilde Sansò. 2011. "An Analytical Model for Jitter in IP Networks." *Annals of Telecommunications* 67 (May): 81–90. <https://doi.org/10.1007/s12243-011-0254-y>.

- Dassault Systemes. 1981. Magic Systems of Systems Architect. Accessed August 27, 2023. <https://www.3ds.com/products-services/catia/products/catia-magic/magic-systems-of-systems-architect/>.
- Dbira, Hadhami, André Girard, and Brunilde Sansò. 2016. "Calculation of Packet Jitter for Non-Poisson Traffic." *Annals of Telecommunications* 71 (January): 223–237. <https://doi.org/10.1007/s12243-016-0492-0>.
- Defense & Aerospace Competitive Intelligence Service. 2019. Budget Line Item Justification: PB 2020 Navy. https://www.dacis.com/budget/budget_pdf/FY20/PROC/N/2960_68.pdf.
- Defense Acquisition University. n.d.a. "Architecture Design Processes." Accessed October 17, 2023. <https://www.dau.edu>.
- Defense Acquisition University. n.d.b. "Performance Attributes." Accessed October 17, 2023. <https://www.dau.edu/acquipedia-article/performance-attributes>.
- Defense Acquisition University. n.d.c "Inherent Availability." Accessed November 01, 2023. <https://www.dau.edu/index.php/glossary/inherent-availability>.
- Defense Industry Daily Staff. 2011. "The Virtual Armed Forces: U.S. Military Turns to Virtualization." August 15, 2011. <https://www.defenseindustrydaily.com/dod-virtual-machines-06991/>.
- Defense Information Systems Agency. 2022. Enclave Test and Development (T&D) Security Technical Implementation Guide (STIG) Overview. <https://public.cyber.mil/stigs/downloads/>.
- Department of Defense. 2014. *Cybersecurity*. DOD Instruction 8500.01. Washington, DC: Department of Defense.
- Department of Defense. 2016. *DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*. DOD Instruction 5200.01. Washington, DC: Department of Defense.
- Department of Defense. 2019. *DOD Digital Modernization Strategy DOD Information Resource Management Strategic Plan FY19-23*. Washington, DC: Department of Defense. <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>
- Department of Defense. 2022. *Risk Management Framework for DOD Systems*. DOD Instruction 8510.01. Washington, DC: Department of Defense.

- Director, Operational Test & Evaluation. 2020. "FY20 Army Program: Integrated Tactical Network (ITN)." The Office of the Director, Operational Test and Evaluation. <https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/army/2020itn.pdf?ver=-3GRf6wR9GagCdAbJI-bsw%3D%3D>.
- EcoSys. 2022. "Earned Value Management: EVM Basics." <https://www.ecosys.net/knowledge/earned-value-management-basics/>.
- Faisandier, Alan and Garry Roedler. n.d. "Stakeholder Needs Definition." SEBoK: Guide to the Systems Engineering Body of Knowledge. https://sebokwiki.org/wiki/Stakeholder_Needs_Definition.
- Fortinet. n.d. "What is Transmission Control Protocol TCP/IP?" Accessed October 04, 2023. <https://www.fortinet.com/resources/cyberglossary/tcp-ip>.
- Froehlich, Andrew. 2021. "Bandwidth (Network Bandwidth)." TechTarget. May 2021. <https://www.techtarget.com/searchnetworking/definition/bandwidth>.
- Geeksforgeeks. 2023. "User Datagram Protocol." May 11, 2023. <https://www.geeksforgeeks.org/user-datagram-protocol-udp/>.
- Hac, Anna. n.d. *On the Modeling of Shared Resources by Queueing Networks with Serialization Delays*. <https://digitalassets.lib.berkeley.edu/techreports/ucb/text/CSD-83-153.pdf>.
- High Performance Computing Modernization Program. 2016. "HPCMP Annual Report." DOD High Performance Computing Modernization Program. <https://apps.dtic.mil/sti/pdfs/AD1051131.pdf>.
- High Performance Computing Modernization Program. n.d. "Who We Are." DOD High Performance Computing Modernization Program. Accessed October 17, 2023. <https://www.hpc.mil/>.
- Hornig, Charles. 1984. "A Standard for the Transmission of IP Datagrams over Ethernet Networks." Internet Engineering Steering Group (IESG). <https://www.rfc-editor.org/rfc/rfc894>.
- Imagine That. 1987. ExtendSim, 10.1.0. Accessed September 16, 2023. <https://extendsim.com/>.
- Infinera. 2020. *Low Latency – How Low Can You Go?* <https://www.infinera.com/wp-content/uploads/Low-Latency-How-Low-Can-You-Go-0188-WP-RevB-0920.pdf>.
- Information Sciences Institute. 1981. "Internet Protocol: DARPA Internet Program Protocol Specification." September 1981. <https://datatracker.ietf.org/doc/html/rfc791>.

- Institute of Electrical and Electronics Engineers. 2008.” IEEE Standard for Information Technology--Telecommunications and Information Exchange Between Systems--Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.” <https://standards.ieee.org/ieee/802.3/4227/>.
- Joint Staff Public Affairs. 2015. *Joint Staff J7 Cyberspace Environment Division/ Joint Information Operations Range*. Hampton Roads, VA: Joint Staff Public Affairs. https://www.itea.org/images/pdf/conferences/2016%20Cyber/Proceedings/ROMERO_CED_JIOR_101.pdf.
- Joint Task Force. 2020. NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations.” <https://doi.org/10.6028/NIST.SP.800-53r5>.
- Kumar, Anurag, D. Manjunath, Joy Kuri. 2008. *Wireless Networking*. Amsterdam: Morgan Kaufmann Publishers. <https://doi.org/10.1016/B978-012374254-4.50008-9>.
- Kurose, James F. and Keith W. Ross. 2013. *Computer Networking: A Top-Down Approach*. London, England: Pearson Education. <https://books.google.com/books?id=fWg5pwAACAAJ>.
- LaGrone, Sam. 2023. “DDG(X) \$122M Land-Based Test Site Opens in Philadelphia.” USNI News. March 22, 2023. <https://news.usni.org/2023/03/22/ddgx-122m-land-based-test-site-opens-in-philadelphia>.
- Law, Averill M. 2015. *Simulation Modeling and Analysis*. 5th ed. New York, NY: McGraw-Hill Education.
- Lopez, C. Todd. 2022. “DOD Releases Path to Cyber Security Through Zero Trust Architecture.” U.S. Department of Defense. <https://www.defense.gov/News/News-Stories/Article/Article/3229211/dod-releases-path-to-cyber-security-through-zero-trust-architecture/>.
- Mozilla Developer Network Web Docs. 2023. “Understanding Latency.” July 4, 2023. https://developer.mozilla.org/en-US/docs/Web/Performance/Understanding_latency.
- National Aeronautics and Space Administration. n.d. “Product Validation.” Accessed November 17, 2023. <https://www.nasa.gov/reference/5-4-product-validation/>.
- National Institute of Standards and Technology. n.d. “Authorize Processing.” Accessed October 17, 2023. https://csrc.nist.gov/glossary/term/authorize_processing.

- Naval Sea Systems Command. n.d.a. “Warfare Centers NSWC Port Hueneme Division: Supporting the Surface Fleet.” <https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Port-Hueneme/What-We-Do/In-Service-Engineering/>.
- Naval Sea Systems Command. n.d.b. “Warfare Centers NSWC Port Hueneme Division: Surface Warfare Engineering Facility.” <https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Port-Hueneme/What-We-Do/Test-Evaluation/SWEF/>.
- Naval Sea Systems Command. n.d.c. “Warfare Centers: What We Do.” <https://www.navsea.navy.mil/Home/Warfare-Centers/What-We-Do/>.
- Naval Surface Warfare Center Dahlgren Division Corporate Communications. 2021. “NSWC Dahlgren Division Supports Virtualized Testing Environment for AN/SPY-6 Radar.” Naval Sea Systems Command. June 25, 2021. <https://www.navsea.navy.mil/Media/News/Article/2671865/nswc-dahlgren-division-supports-virtualized-testing-environment-for-anspy-6-radar/>.
- Network Playroom. 2017. “CCIE 400–101: Network Principles – Latency, Windowing, BDP, Global Synchronization.” August 5, 2017. <https://www.networkplayroom.com/2017/08/ccie-400-101-network-principles-latency.html>.
- Open Control. n.d. “Steps of the ATO Process.” Accessed November 04, 2023. <https://atos.open-control.org/steps/>.
- Oppenheimer, Priscilla. 2011. *Top-Down Network Design*. Indianapolis, IN: Cisco Press. O’Reilly.
- Ottis, Rain and Peeter Lorents. 2010. “Cyberspace: Definition and Implications.” In *Academic Conferences International Limited: 267-XII*. <https://www.proquest.com/openview/11c3f4f3a7ca044eeb3a18a4929dc5ff/1?pq-origsite=gscholar&cbl=396500>.
- Pedersen, Kjartan, Jan Emblemståg, Reid Bailey, Janet K. Allen, and Farrokh Mistree. 2000. “Validating Design Methods & Research: The Validation Square.” In *Proceedings of DETC ‘00 2000 ASME Design Engineering Technical Conferences: 1–13*. https://www.researchgate.net/publication/238355807_The%27%27Validation_Square%27%27-Validating_Design_Methods.
- Page, Christopher J., and Jean D. Reese. 1996. “Networking Requirements Analysis for Engineering 2000.” Master’s thesis, Naval Postgraduate School. <https://calhoun.nps.edu/handle/10945/8731>.
- Quick, Holly. 2021. “Navy Center for Advanced Modeling and Simulation.” The Department of the Navy’s information technology magazine. June 2021. <https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=2297>.

- Ramaswamy, Ramaswamy, Ning Weng, and Tilman Wolf. 2004. Characterizing Network Processing Delay. 0–7803-8794-5/04. IEEE Communications Society Globecom. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1378257>.
- Real-Time Innovations, Inc. 2007. *Meeting Real-Time Requirements in Integrated Defense Systems*. Sunnyvale, CA. https://d2vkrkwbbxbylk.cloudfront.net/sites/default/files/archive/Real-Time_Integrated_Defense_Systems.pdf.
- Rhoades Jr, Clifford E. 2008. “Department of Defense High Performance Computing Modernization Program. 2007 Annual Report.” March 2008. <https://apps.dtic.mil/sti/tr/pdf/ADA487505.pdf>.
- Risk, Erin. 2021. “TCP vs. UDP: When to Use Which Protocol.” *Twingate Blog*, December 2, 2021. <https://www.twingate.com/blog/tcp-vs-udp>.
- Rockwell Automation. n.d. “System Availability.” Accessed November 01, 2023. <https://fiixsoftware.com/glossary/system-availability/>.
- Roesener, August G., Carl Bottolfson, and Gerry Fernandez. 2014. “Policy for U.S. Cybersecurity.” *Air & Space Power Journal* (Winter): 38–54.
- Russell, William. 2021. Weapon Systems Cybersecurity: Guidance Would help DOD Programs Better Communicate Requirements to Contractors. GAO-21-179. Washington, DC: Government Accountability Office.
- Salehin, Khondaker M. and Roberto Rojas-Cessa. n.d. *Scheme for Measuring Queueing Delay of a Router Using Probe-Gap Model: The Single-Hop Case*. <https://web.njit.edu/~rojasces/publications/khoroCL14.pdf>.
- Schurgot, Dr. Mary R. 2021. “Mission-Integrated Network Control (MINC).” Defense Advanced Research Projects Agency (DARPA). <https://www.darpa.mil/program/mission-integrated-network-control>.
- Systems Engineering Department. n.d. *Systems Engineering Guide: System Life Cycle Process Models – Vee Diagram*. https://02f0a56ef46d93f03c90-22ac5f107621879d5667e0d7ed595bdb.ssl.cf2.rackcdn.com/sites/785/uploads/7258/System_Life_Cycle_Vee_Process_Model_Guide20151007-14347-13vz9n1.pdf.
- Taylor, Petroc. 2023. “Average Mobile and Fixed Broadband Download and Upload Speeds Worldwide as of April 2023.” Statista. June 1, 2023. <https://www.statista.com/statistics/896779/average-mobile-fixed-broadband-download-upload-speeds/>.
- Test Resource Management Center. 2019. “Joint Mission Environment Test Capability (JMETC) Program Overview.” June 2019. <https://www.trmc.osd.mil/attachments/JMETC-OverviewBrief-2019-06-05-DistA.pdf>.

- Umenne, Patrice O., and Marcel O. Odhiambo. 2013. "Performance Analysis of a WiMAX/WiFi System Whilst Streaming a Video Conference Application." *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering* 7 (7): 846–850. Scholar Waset.
- United States Department of Commerce. 2004. Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. Gaithersburg, MD. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>.
- United States Department of Defense Chief Information Office Cybersecurity Architecture Division. 2023. *Department of Defense (DOD) Cybersecurity Reference Architecture*. Washington, DC: Office of Republication and Security Review. <https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf>.
- United States Department of Defense. 2017. "Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs." Washington, D.C., <https://acqnotes.com/wp-content/uploads/2017/07/DOD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf>.
- United States Department of Defense Chief Information Officer. n.d. "DoDAF DOD Architecture Framework Version 2.02 DOD Deputy Chief Information Officer: Architecture Development." Accessed October 17, 2023. https://dodcio.defense.gov/Library/DOD-Architecture-Framework/dodaf20_arch_development/.
- Walden, David D., Garry J. Roedler, Kevin J. Forsberg, R. Douglas Hamelin, and Thomas M. Shortell. 2015. *INCOSE: Systems Engineering Handbook*. 4th ed. Hoboken, New Jersey: John Wiley & Sons, Inc.
- Zenarmor. 2023. "What is the Advanced Encryption Standard (AES)?" October 9, 2023. <https://www.zenarmor.com/docs/network-security-tutorials/what-is-advanced-encryption-standard-aes#:~:text=AES%20Algorithm%20Used?-,%E2%80%8B,organizations%2C%20to%20secure%20sensitive%20data.>

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE