



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**A REPEATABLE THREAT-BASED REQUIREMENTS
GENERATION PROCESS LEVERAGING MODEL-BASED
SYSTEMS ENGINEERING FOR JOINT EXPLOSIVE
ORDNANCE DISPOSAL AND AN ANALYSIS OF RAPID
LARGE AREA CLEARANCE**

by

Angel M. Gill

September 2022

Thesis Advisor:
Co-Advisor:

John M. Green
Bonnie W. Johnson

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 September 2022	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE A REPEATABLE THREAT-BASED REQUIREMENTS GENERATION PROCESS LEVERAGING MODEL-BASED SYSTEMS ENGINEERING FOR JOINT EXPLOSIVE ORDNANCE DISPOSAL AND AN ANALYSIS OF RAPID LARGE AREA CLEARANCE			5. FUNDING NUMBERS	
6. AUTHOR(S) Angel M. Gill				
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) The mission of the Joint Explosive Ordnance Disposal (JEOD) program is to reduce or eliminate explosive hazards that jeopardize personnel, operations, installations, or materiel. The JEOD program develops equipment in support of this mission. The equipment development begins with identification of a threat. JEOD has a defined process for threat analysis and capability gap assessment but lacks a process for the generation of system requirements for the Joint Capabilities Integration and Development System (JCIDS). This thesis studied the shortcomings of the current JEOD requirements generation process and developed a new repeatable threat-based process based on a comprehensive review of systems engineering requirements processes. The new JEOD requirements process incorporates model-based systems engineering (MBSE) to analyze the threat and capability gaps and translate them into quantifiable requirements. The thesis applied this new process using MBSE tools and Monterey Phoenix behavior modeling to the JEOD mission of Rapid Large Area Clearance (RLAC) as a case study to identify common mission scenarios and stakeholder requirements that can be used to develop system requirements. The new process can be used for future JEOD requirements development to reduce the burden on JEOD technicians, shorten the requirements development timeline, and produce more comprehensive and accurate requirements. The new process is extensible to the broader DOD requirements generation community.				
14. SUBJECT TERMS requirements, Joint Explosive Ordnance Disposal, JEOD, joint service, JCIDS, rapid large area clearance, threat based requirements, requirements validation, quantifiable requirements, model-based systems engineering, MBSE, Monterey Phoenix			15. NUMBER OF PAGES 189	
			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	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**A REPEATABLE THREAT-BASED REQUIREMENTS GENERATION
PROCESS LEVERAGING MODEL-BASED SYSTEMS ENGINEERING FOR
JOINT EXPLOSIVE ORDNANCE DISPOSAL AND AN ANALYSIS OF RAPID
LARGE AREA CLEARANCE**

Angel M. Gill
Civilian, Department of the Navy
BS, West Virginia University, 2001
MS, West Virginia University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
September 2022**

Approved by: John M. Green
Advisor

Bonnie W. Johnson
Co-Advisor

Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The mission of the Joint Explosive Ordnance Disposal (JEOD) program is to reduce or eliminate explosive hazards that jeopardize personnel, operations, installations, or materiel. The JEOD program develops equipment in support of this mission. The equipment development begins with identification of a threat. JEOD has a defined process for threat analysis and capability gap assessment but lacks a process for the generation of system requirements for the Joint Capabilities Integration and Development System (JCIDS). This thesis studied the shortcomings of the current JEOD requirements generation process and developed a new repeatable threat-based process based on a comprehensive review of systems engineering requirements processes. The new JEOD requirements process incorporates model-based systems engineering (MBSE) to analyze the threat and capability gaps and translate them into quantifiable requirements. The thesis applied this new process using MBSE tools and Monterey Phoenix behavior modeling to the JEOD mission of Rapid Large Area Clearance (RLAC) as a case study to identify common mission scenarios and stakeholder requirements that can be used to develop system requirements. The new process can be used for future JEOD requirements development to reduce the burden on JEOD technicians, shorten the requirements development timeline, and produce more comprehensive and accurate requirements. The new process is extensible to the broader DOD requirements generation community.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	2
B.	PROBLEM STATEMENT	4
C.	OBJECTIVES	4
D.	THESIS APPROACH	5
E.	THESIS ORGANIZATION.....	6
 II.	 LITERATURE REVIEW	 7
A.	REQUIREMENTS GENERATION GUIDANCE	8
1.	Requirements Generation in Product Design.....	8
2.	Role of Requirements Generation in Systems Engineering	10
3.	Commercial Guidance	17
4.	DOD Specific Guidance.....	19
5.	Take-Aways from the Review of Requirements Generation Processes	26
B.	MODEL-BASED SYSTEMS ENGINEERING	27
1.	Role in Systems Engineering Requirements Generation	27
2.	MBSE Tools.....	28
 III.	 GENERATION OF JOINT EXPLOSIVE ORDNANCE DISPOSAL REQUIREMENT PROCESS	 29
A.	ANALYSIS OF THE EXISTING JEOD REQUIREMENTS PROCESS	31
1.	Identifying Stakeholders	31
2.	Identifying Enabling Processes	39
3.	Gathering Stakeholder Needs	44
4.	Prioritizing Stakeholder Needs	44
5.	Developing Operational Scenarios	46
6.	Defining Interactions of System.....	46
7.	Identifying Constraints.....	55
8.	Developing Stakeholder Requirements.....	56
9.	Developing Measures of Effectiveness (MOEs) and Measures of Suitability (MOSS).....	56
10.	Analyzing Requirements	58
11.	Recording in Database.....	58
B.	DEVELOPMENT OF NEW JEOD REQUIREMENTS PROCESS	59

1.	Process Boundary.....	59
2.	Changes to Existing Process Steps.....	59
3.	Comparison of New Process Timeline to Old.....	73
IV.	RAPID LARGE AREA CLEARANCE REQUIREMENTS ANALYSIS.....	77
A.	STAKEHOLDER NEEDS ANALYSIS	78
1.	Identifying Stakeholders	78
2.	Identifying Enabling Systems and Processes.....	79
3.	Gathering Stakeholder Needs	84
4.	Prioritizing Stakeholder Needs.....	90
5.	Developing Operational Scenarios	91
6.	Defining Interactions of System.....	93
7.	Identifying Constraints.....	94
8.	Developing Stakeholder Requirements.....	94
9.	Defining RLAC Measures of Effectiveness and Measures of Suitability	97
10.	Analyzing Stakeholder Requirements.....	98
B.	SYSTEM REQUIREMENTS ANALYSIS	100
1.	Generating Plan for Defining System Requirements	100
2.	Establishing System Boundary and Interaction with External Systems.....	100
3.	Identifying and Defining the Required System Functions	101
4.	Proposing a Physical Architecture	102
5.	Identifying Constraints on System	104
6.	Identifying Critical Characteristics.....	104
7.	Identifying Technical Risks.....	105
8.	Generating System Requirements	107
9.	Analyzing System Requirements	108
V.	CONCLUSION	111
A.	SUMMARY OF RESULTS	111
1.	Objective One Results.....	112
2.	Objective Two Results	113
3.	Objective Three Results	114
B.	RECOMMENDATIONS.....	114
1.	Recommendation 1 – New Requirements Process Leveraging MBSE.....	115
2.	Recommendation 2 – JEOD Program Requirements Roles and Tasks.....	115
3.	Recommendation 3 – RLAC Approach	115

C. FUTURE WORK.....	116
APPENDIX A. INNOSLATE MODELS	117
APPENDIX B. JEOD AND RLAC DATA	125
APPENDIX C. MONTEREY PHOENIX CODE AND RESULTS	141
LIST OF REFERENCES.....	157
INITIAL DISTRIBUTION LIST	163

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Thesis Steps Taken	5
Figure 2.	Chapter II Steps.....	7
Figure 3.	Needs to Goals Framework. Source: Crawley, Cameron, and Selva (2016).	9
Figure 4.	Requirements Pyramid. Source: Buede and Miller (2016, 148).	12
Figure 5.	Role of CONOPS in Requirements Generation. Source: Week (2015).	13
Figure 6.	Dual Vee Model. Source: Mooz, Hal, and Forsberg (2006).	14
Figure 7.	Types of Requirements. Source: ISO/IEC/IEEE 29148:2011E (2018).	15
Figure 8.	Systems Engineering V-Model. Source: Roedler and Jones (2005).	16
Figure 9.	Example of an Epic Story. Source: Kitowska (2022).	18
Figure 10.	JCIDS Process Overview. Source: Intellipedia (2021).	23
Figure 11.	JCIDS Document Sequences. Source: Intellipedia (2021).	24
Figure 12.	Chapter III Steps Taken	29
Figure 13.	DOD SE Process Model of 2014. Source: DAU (2014).	30
Figure 14.	JEOD Stakeholders	33
Figure 15.	JCIDS Deliberate CDD Staffing (103 days). Source: Intellipedia (2021).	38
Figure 16.	Systems Engineering Combined Model. Adapted from Hitchins (2007).	40
Figure 17.	Current JEOD Process Asset Hierarchy Chart.....	42
Figure 18.	Current JEOD Process Hierarchy Chart	43
Figure 19.	Stakeholder Analysis	45
Figure 20.	Existing JEOD Requirements Process	47

Figure 21.	Example Monterey Phoenix Code ROOT Threat SME.....	51
Figure 22.	New JEOD Requirements Process Top Level	59
Figure 23.	New Capability Gap Definition Process	60
Figure 24.	New Step to Generate MBSE Scenarios	60
Figure 25.	Modified Threat Expo Process.....	62
Figure 26.	Modified Technology Demonstrations	63
Figure 27.	Modified IPCL Process.....	64
Figure 28.	New Requirements Generation Process Step.....	65
Figure 29.	Modified Enclosure F Process	66
Figure 30.	Develop Stakeholder Requirements Steps	67
Figure 31.	Define MOEs and MOSs Steps.....	68
Figure 32.	Analyze Stakeholder Requirements	69
Figure 33.	Modified Charter RWG Process	70
Figure 34.	Modifications to Write Documents Process	72
Figure 35.	Comparison of Timelines.....	75
Figure 36.	Chapter IV Steps Taken	77
Figure 37.	RLAC Enabling Technologies	80
Figure 38.	The Robots Deployed. Source: Malatesta (2021).	82
Figure 39.	USN UUV Plans. Source: Malatesta (2021).....	83
Figure 40.	Stakeholder Process Needs and JCIDS CDD Alignment	86
Figure 41.	Stakeholder RLAC Needs and JCIDS CDD Alignment.....	88
Figure 42.	RLAC Functions	89
Figure 43.	RLAC Constraints.....	89
Figure 44.	RLAC Concept of Operations.....	93
Figure 45.	RLAC Stakeholder Requirement Types	96

Figure 46.	RLAC System Asset Diagram	100
Figure 47.	RLAC Functions by Task Area.....	101
Figure 48.	RLAC Functions by Process Area	102
Figure 49.	RLAC Physical Architecture by Task Area.....	102
Figure 50.	RLAC Physical Architecture by Process Area	103
Figure 51.	MP Trace for RLAC Maximum Area Scanned	106
Figure 52.	MP Trace RLAC Maximum Hazards Found	107
Figure 53.	Thesis Steps Taken	112
Figure 54.	Current Threat Analysis Process.....	117
Figure 55.	Current Capability Gap Definition Process	117
Figure 56.	Current Existing Requirements Generation Process.....	117
Figure 57.	Current JCIDS Validation Process.....	118
Figure 58.	JCIDS CDD Mapping	119
Figure 59.	JEOD Process Stakeholder Requirements	120
Figure 60.	JEOD Process Requirements Traceability Matrix	121
Figure 61.	RLAC Requirements Traceability Part 1	122
Figure 62.	RLAC Requirements Traceability Part 2.....	123
Figure 63.	Lines 1–25: Title, Description, References.....	141
Figure 64.	Lines 26–61: SCHEMA, ROOTS MTAB and Threat SME.....	141
Figure 65.	Lines 62–95: ROOT Project Management	142
Figure 66.	Lines 96–114: ROOT Office of Naval Research.....	142
Figure 67.	Lines 115–160 ROOT Requirements Writer	143
Figure 68.	Lines 161–212: COORDINATE Requirements Writer	144
Figure 69.	Lines 213–222: Mark Traces That Have All Sections Completed to Complete the CDD.....	145

Figure 70.	Lines 223–275: Risk of CDD Not Completed (1)	145
Figure 71.	Lines 276–325: Risk of CDD Not Completed (2)	146
Figure 72.	Lines 326–330: Risk of CDD Not Completed (3)	146
Figure 73.	Lines 331–373: Risk Table and Summary	147
Figure 74.	Lines 380–399: Calculate Total Risk.....	147
Figure 75.	Trace 1: CDD Completed	148
Figure 76.	Trace 2: AoA Not Provided. CDD Not Completed.	148
Figure 77.	Trace 3: Acquisition Plan Not Provided. CDD Not Completed.	148
Figure 78.	Trace 4: Acquisition Plan and AoA Not Provided. CDD Not Completed.	149
Figure 79.	Trace 5: Threat Summary Not Provided. CDD Not Completed.	149
Figure 80.	Trace 6: Threat Summary and AoA Not Provided. CDD Not Completed.	150
Figure 81.	Trace 7: Threat Summary and Acquisition Plan Not Provided. CDD Not Completed.	150
Figure 82.	Trace 8: Threat Summary, Acquisition Plan, and AoA Not Provided. CDD Not Completed.....	151
Figure 83.	Trace 9: CONOPS Not Provided. CDD Not Completed.	151
Figure 84.	RLAC MP Code Lines 1–39.....	152
Figure 85.	RLAC MP Code Lines 40–91	153
Figure 86.	RLAC MP Code Lines 92–137.....	154
Figure 87.	RLAC MP Code Lines 138–163.....	155
Figure 88.	RLAC MP Code Lines 164–196.....	155
Figure 89.	RLAC MP Code Lines 197–238.....	156
Figure 90.	RLAC MP Code Lines 239–254.....	156

LIST OF TABLES

Table 1.	INCOSE Requirements Steps. Adapted from Walden et al. (2015).	11
Table 2.	JEOD Stakeholders	31
Table 3.	Current JEOD Requirement Generation Timeline.....	48
Table 4.	Write Requirement Document Timeline.....	48
Table 5.	JCIDS CDD Required Documents with Stakeholders.....	50
Table 6.	Event Risks for MP Trace 1 CDD	53
Table 7.	CDD Completion Trace Probability	54
Table 8.	Comparison of New and Current JEOD Requirement Generation Timeline	73
Table 9.	Detailed Comparison of Current and New Requirement Document Timelines.....	74
Table 10.	JEOD Stakeholders	78
Table 11.	RLAC System Constraints.....	94
Table 12.	JEOD Stakeholder Needs.....	125
Table 13.	JEOD to Product Development Comparison	126
Table 14.	JEOD to Needs and Goals Comparison	127
Table 15.	JEOD to INCOSE Comparison.....	128
Table 16.	JEOD to DOD SE Comparison.....	129
Table 17.	JEOD to Agile Comparison	130
Table 18.	Current JEOD Process Constraints	131
Table 19.	JCIDS DoDAF Connections	131
Table 20.	RLAC Stakeholder Needs.....	137

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AEODRS	advanced EOD robotic system
AoA	analysis of alternatives
APAs	additional performance attributes
AV	all viewpoint
CBA	capabilities-based assessment
CBRN	chemical, biological, radiological, nuclear
CBVM	capabilities-based value model
CDD	capabilities development document
CIPs	critical intelligence parameters
CONOPS	concept of operations
CR	capability requirement
CUI	controlled unclassified information
CV	capability viewpoint
DAG	defense acquisition guidebook
DCR	DOTmLPF-P change recommendation
DIV	data and information viewpoint
DOD	Department of Defense
DODAF	Department of Defense architecture framework
DOTmLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities - policy
DSS	decision support system
E3	electromagnetic environmental effects
EOD	Explosive Ordnance Disposal
ERB	Equipment Review Board
FCB	Functional Capabilities Board
FlexCSR	flexible cyber-secure radio
FOC	full operational capability
FoS	family of systems
FRD	functional requirements document
FRS	future radiographic system

ICD	initial capabilities document
IEDs	improvised explosive devices
INCOSE	International Council on Systems Engineering
IOC	initial operational capability
IS	information system
IPCL	integrated prioritized capabilities list
JCB	Joint Capabilities Board
JCIDS	Joint Capabilities Integration and Development System
JEOD	Joint Explosive Ordnance Disposal
JEOD T and T	Joint Explosive Ordnance Disposal Technology and Training
KPPs	key performance parameters
KSAs	key systems attributes
KW	kilo watt
MBSE	model-based systems engineering
MCM	maritime expeditionary countermeasures
MEASUR	method for eliciting analyzing and specifying user' requirements
MEMUUV	maritime expeditionary MCM unmanned undersea vehicle
MESR	maritime expeditionary standoff response
MOEs	measures of effectiveness
MOSs	measures of suitability
MP	Monterey Phoenix
MRAP	mine-resistant ambush protected
MTA	middle tier acquisition
MTAB	Military Technical Acceptance Board
MTCD	middle tier capability document
MTRS	man transportable robotic system
NAVSCOLEOD	Naval School Explosive Ordnance Disposal
NPS	Naval Postgraduate School
OMS/MP	operational mode summary/mission profile
ONR	Office of Naval Research
OPNAV	Chief of Naval Operations
OV	operational viewpoint

RADAS	rapid airfield damage assessment system
RADBO	recovery of airbase denied ordnance
RISEOD	radiographic imaging system for EOD
RLAC	rapid large area clearance
RWG	requirements working group
SE	systems engineering
SME	subject matter expert
SOIL	sub-surface ordnance and IED locator
SoN	statement of need
SoS	system of systems
SRSD	standoff render safe and disrupt
SysML	systems modeling language
StdV	standard viewpoint
SV	systems viewpoint
TLR	top level requirements
TPMs	technical performance measures
TRL	technology readiness level
TTAB	Training Technical Acceptance Board
UAS	unmanned aerial system
UAV	unmanned ariel vehicle
UGV	unmanned ground vehicle
UUV	unmanned underwater vehicle
UJT	universal joint task
USAF	United States Air Force
USMC	United States Marine Corps
USN	United States Navy
UXO	unexploded ordnance
VOLT	validated online life cycle report

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Joint Explosive Ordnance Disposal (JEOD) program has a need to quickly develop comprehensive and effective requirements to meet emerging threats. This thesis used model-based systems engineering (MBSE) to analyze the current process employed to develop requirements. The analysis showed that the current process is a serial process that currently takes around 2 years to validate a single requirements document in the Joint Capabilities Development and Integration System (JCIDS). The analysis also showed that the current process does not break down the steps to generate requirements documents in enough detail to produce quantifiable requirements that trace back to threats. Rather, the requirements are produced in a qualitative fashion which repeats for each new capability gap.

The thesis used a behavioral modeling software called Monterey Phoenix to analyze the current process and discovered that one of the key missing components was the generation of a concept of operation (CONOPS) for the system in regard to the capability gap. There was also limited data gathered for relevant technologies and program strategy. The current process did not follow systems engineering guidelines. This caused key stakeholder needs to be missed which led to requirements documents that were not validated or did not result in fielded systems.

In order to resolve these issues, an extensive literature review of systems engineering guidance documents, agile requirements development, and the JCIDS process was conducted. This information was synthesized to develop a new process based on MBSE with the goals of being repeatable, threat-based, and timely. Portions of the current process which worked well were retained. Systems engineering rigor was added and the new process was modeled in Innoslate. Inputs and outputs were shown for each step, and the association between the Department of Defense Architecture Framework (DODAF) views to each step of the Capabilities Development Document (CDD) were highlighted.

The new process is based on capturing stakeholder needs and tracking them through the entire process to allow for traceability. The process develops mission scenarios, or

CONOPs to support the development and analysis of requirements. The threats and CONOPS are tracked throughout the process to ensure alignment with the requirements.

The thesis performed an analytical comparison of the new requirements generation process timeline to the current process. The analysis showed that the new process takes approximately 1.5 years versus the current process taking 2 years. Additionally, the analysis indicated that several of the steps in the new process to develop the CONOPS and MBSE diagrams were started earlier in the process which allowed a second requirements document to be finished within the original two-year time frame. This effectively doubled the number of requirements documents that could be produced.

The thesis used the new requirements generation process to develop stakeholder requirements and propose an architecture to address the emerging threat of rapid large area clearance (RLAC). During the generation of the requirements, relevant requirements documents were reviewed to create a requirements database that could be used for future JEOD efforts. Common mission areas and stakeholder needs were identified that could be used on future efforts.

The thesis demonstrated that the use of MBSE adds value to the development of requirements by creating a process based on system engineering principles that is repeatable, based on threat analysis, saves time, and produces more comprehensive and effective requirements based on stakeholder needs. Additionally, the use of Monterey Phoenix was able to identify overly constrained requirements. The thesis shows that this process is critical for the JEOD program and can be used immediately to develop requirements for the RLAC mission. Moreover, the process shows potential benefits for a wider adoption in DOD programs—especially those with changing and evolving threats. The thesis recommends additional research into this new requirements generation process to include continued work on developing RLAC requirements, application to additional JEOD missions, and investigation into whether this process could be adopted earlier in the JEOD process to reduce the timeline and streamline the process of fielding much-needed equipment and systems.

ACKNOWLEDGMENTS

This work could not have been completed without the help and support of multiple individuals. First and foremost, my family, who listened to all my ideas and provided encouragement. Without their understanding and patience, the many hours that went into this work could not have been accomplished.

My PD-21 classmates became like a second family and provided a sounding board for ideas. I learned to look at the world from a different point of view with their help and came up with many great ideas outside of the scope of this document.

Outside of the PD-21 cohort, there were two teams that provided help with sections of this work. The first was the Hazardous 5 Team, consisting of Geoffry Eberle, Alexander Fedorovich, Andrew Machamer, and Mary Mesa. They contributed to the Monterey Phoenix program, which analyzed rapid large area clearance in Chapter IV. Also in Chapter IV, Alain Francois Mbateng Tchuisseu, Joseph Grim, Christy Spaulding, and Allen Zahneigh helped develop CONOPS and stakeholder needs for rapid large area clearance.

The work in Chapters III and Chapters IV could not have been accomplished without the help of Kristin Giammarco for Monterey Phoenix and instruction on Innoslate.

And finally, my advisors, who met with me regularly and provided the encouragement, constructive feedback, and direction to keep this thesis on track.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Requirements generation is a key part of the system engineering process. When written correctly, requirements can result in the development and implementation of a solution that satisfies the original need. When written incorrectly, requirements can result in solutions that may not meet the original need, cause schedule delays, budget overruns, and potentially cancellation of the effort.

Due to this, there has been extensive research and guidance published on how to develop requirements as part of the system engineering process. These include the “Systems Engineering Body of Knowledge” (SEBoK 2021), *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities* (Walden 2015), *Systems and Software Engineering – Life Cycle Processes – Requirements Engineering* (ISO/IEC/IEEE 29148:2011E 2018), and *Guide to Writing Requirements* (INCOSE 2012). These examples are not exhaustive, but a brief list of some of the available guidance on requirements writing.

The Department of Defense (DOD) has adopted many of these methods. They are described in the *Defense Acquisition Guidebook*, which discusses how requirements fit into the acquisition process (DAG 2021), and the *Joint Capabilities Integration and Development System (JCIDS) Manual* (Intellipedia 2021). The *JCIDS Manual* provides the guidance for joint service DOD programs. JCIDS purpose is to ensure requirements are designed to be effective in influencing the resourcing of a capability development through the entire acquisition process. The goal is to, “prevent fielding of capabilities so foundationally flawed it would be inconceivable the cyber risks could be cost effectively mitigated to achieve and maintain an operationally relevant mission risk posture throughout the life cycle” (Intellipedia 2021, 1). All efforts that develop requirements for joint programs must follow the JCIDS guidance. In addition, they should attempt to adhere to the best practices laid out in the systems engineering guidance previously discussed.

This thesis looked at the requirements generation process specific to the Joint Explosive Ordnance Disposal (JEOD) program. Like other DOD programs that develop

materiel and non-materiel solutions, JEOD has a need to develop requirements for the equipment it uses in support of its mission. Since JEOD is Joint service, it has been following the JCIDS process which defined the content required in a requirements document. The JCIDS process did not define how to generate the content for the requirements documents for specific capability gaps. The generation of the content could be done utilizing systems engineering guidance, which was not currently utilized by JEOD. This resulted in requirements that did not effectively meet the JCIDS guidelines causing delays and even cancellations of JEOD efforts. Using a system engineering approach to develop requirements for a specific capability could help JEOD develop effective requirements for validation in JCIDS.

A. BACKGROUND

The Explosive Ordnance Disposal (EOD) program first came into existence when the British Royal Navy dismantled/recovered the first German magnetic mine in 1939 (NAVSEA 2021). In the years afterwards, the program grew and spread to the United States.

The EOD program mission “is to enable accomplishment of the joint force and/or the geographic combatant commander’s mission objectives in support of U.S. national security by maintaining access to areas denied by explosive ordnance to facilitate awareness of the operational environment, force protection, operational mobility, and maneuver” (CJCS 2016, vii).

Each service had their own branch of EOD and in 1951 the United States Navy was assigned joint service EOD responsibility for basic training, research, and development to avoid duplication of effort. Currently, DOD Directive 5160.62 designates the Secretary of the Navy as Executive Manager for JEOD. DOD Directive 5160.62 also establishes a Program Board which is made up of flag/general officers. One from each of the four services. Their role is to represent each of their individual services and provide service feedback to the Executive Manager. Therefore, all decisions made at the Program Board level must be agreed upon by each of the four services (DOD Directive 5160.62 2021). While each service retained their individual EOD programs, they were required to send

representatives to JEOD to ensure that there was consistency across the programs and to reduce or eliminate duplication of effort.

Until the wars in Iraq and Afghanistan, the EOD mission was focused mainly on unexploded ordnance such as mines and bombs. The Iraq and Afghanistan wars introduced improvised explosive devices (IEDs) as a new threat to be countered by JEOD.

Currently, both traditional unexploded ordnance (UXO) and IEDs remain threats that JEOD must counter. However, there is also a new threat identified in a RAND study to counter Chinese anti-access strategies (Cliff et al. 2007). Based on the RAND study, anti-access strategies are designed to slow down the U.S. military's ability to operate in remote locations. The RAND study discussed attacks against logistics systems as well as against the air bases and ports used in support of military movement in and out of remote locations. According to the RAND study, China could use runway-penetrating submunitions and high-explosive bomblet submunitions to cover large areas of runways rendering them inoperable. This threat requires JEOD to look for ways not just to perform their mission, but to perform it faster over a larger area.

In order to counter existing and new threats, JEOD has developed a Capabilities-Based Value Model (CBVM) process to analyze threats and determine capability gaps. These capability gaps are then translated into requirements to enter JCIDS for validation into approved joint requirements.

There is not currently a repeatable, threat-based systems engineering process that takes the JEOD capability gaps and translates them into quantifiable requirements for validation in JCIDS. Currently, requirements are written based on qualitative data versus quantitative threat-based data. This results in requirements that are either delayed or do not make it through the validation process, ultimately jeopardizing program and mission success. It has been shown that for requirements that do not make it through the validation process, the process used is not always systems engineering based which results in successive efforts not being able to build on the work previously done (Hoff 2009).

In the past 10 years, JEOD has developed a limited number of Capability Development Documents (CDDs) and very few of them have resulted in successful

programs. The reason JEOD requirements do not make it through validation needs to be understood to prevent future program failures and delays. A tracking system is also required to manage the requirements to help prevent delays and allow for a repeatable process.

While requirements generation for JEOD has been slow, the rapidly changing threats which JEOD faces has continued to evolve. Due to the lack of requirements being produced by JEOD, new development efforts have not been able to be initiated to respond to these evolving threats. A process is needed to allow JEOD to write joint requirements that are able to be produced in a timely manner and properly address the evolving threats that JEOD faces.

B. PROBLEM STATEMENT

Due to the continuously changing threats that JEOD faces, and the need to field equipment rapidly, a process is needed that will allow JEOD to translate identified capability gaps into threat-based requirements. These requirements need to be produced in a timely manner and in a format that can receive approval through the JCIDS process. In particular, requirements are needed for rapid large area clearance to counter the threat posed by Chinese anti-access strategies (Cliff et al. 2007).

C. OBJECTIVES

This thesis had three objectives:

- Objective 1: To develop a requirements generation process for the JEOD program that is repeatable with quantifiable threat-based requirements that can be validated through the JCIDS process.
- Objective 2: To apply this requirements generation process to a JEOD program mission use case (Rapid Large Area Clearance (RLAC)) to develop RLAC system requirements and evaluate the process.
- Objective 3: To evaluate the contribution of model-based systems engineering (MBSE) tools (Innoslate and Monterey Phoenix) to the JEOD program

requirements generation process; specifically, as a method that allows future access to MBSE data and artifacts and allows the generation of future requirements as threats evolve.

D. THESIS APPROACH

This thesis used a system engineering approach to develop a requirements generation process for JEOD and analyze the RLAC need. The approach consisted of four main steps which were shown in Figure 1.

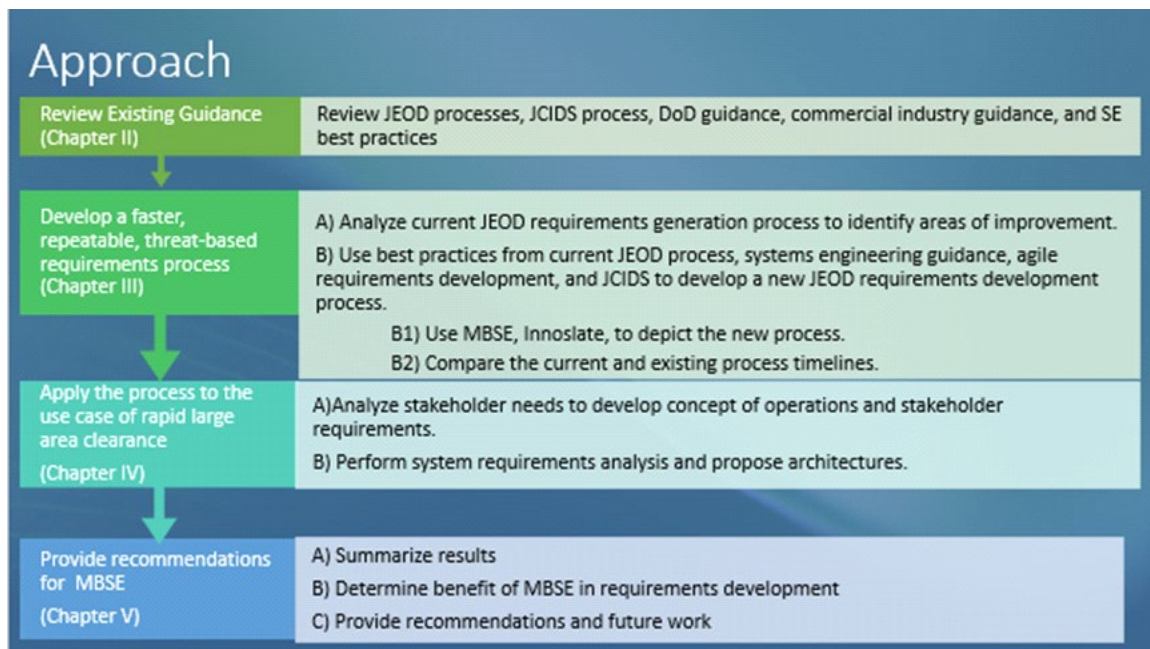


Figure 1. Thesis Steps Taken

For the first step, the existing JEOD threat data process, capability gap determination process, requirements generation process, and the JCIDS process were analyzed to establish the scope and needs of the JEOD community in regard to a requirements generation. In the second step, a new requirements generation process was developed leveraging items from the existing JEOD processes, other DOD guidance, commercial industry best practices, and systems engineering guidance. This satisfied the first objective of the thesis.

For the third step, the requirements generation process was tested by using it to analyze the RLAC need. RLAC needs were compared to past JEOD requirements to identify common mission scenarios and requirements in order to use this same process for future JEOD efforts as well as other DOD efforts. This satisfied the second objective of the thesis.

Finally, in the fourth step, recommendations for the implementation of model-based systems engineering (MBSE) tools such as Innoslate or Monterey Phoenix as well as future work were also provided. This satisfied the third and final objective of the thesis.

E. THESIS ORGANIZATION

This thesis applied systems engineering concepts and methodologies and the document is structured to follow a similar approach. Chapter I presents the problem, defines the scope, and presents the objectives that the thesis must achieve. Chapter II presents the literature review that provides an overview of work already in place with regards to requirements and the use of model-based systems engineering for requirements development and for JEOD. Chapter III describes the analysis of existing JEOD process and development of a new JEOD requirements process. Chapter IV presents the new requirements process to analyze the emerging threat of rapid large area clearance and determined common mission scenarios and requirements for JEOD. Chapter V summarizes the results of Chapters III and IV, provides recommendations, and proposes future work.

II. LITERATURE REVIEW

This chapter summarizes the literature review for this thesis. As shown in Figure 2, the purpose of the literature review was to determine what guidance already existed for requirements generation for JEOD as well as the DOD and commercial industry.

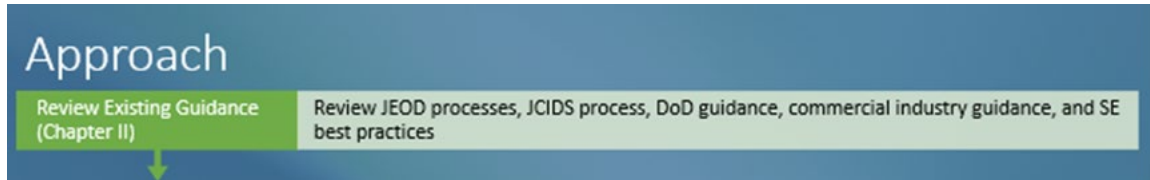


Figure 2. Chapter II Steps

The goal was to leverage existing processes when possible. When there were not existing processes to use, various sets of guidance were reviewed to determine how they could be used to create a new process or integrate with existing processes. Various sources from DOD, commercial industry, and systems engineering guidance were reviewed to determine if there were concepts from each area that could add value to the JEOD requirements process.

The literature review showed that there was no existing documentation that provided an existing process for repeatable threat-based requirements generation for JEOD. There was significant information in various areas that when combined supported development of such a process.

The first part of the literature review looked at how requirements generation is defined in product development, standard systems engineering guidance, DOD guidance, and the requirements processes that commercial industry uses. The second section of the literature review presented material that discussed how model-based systems engineering tools are used for systems engineering requirements development in the DOD, commercial industry, and JEOD.

A. REQUIREMENTS GENERATION GUIDANCE

Since the first objective of the thesis was to develop a new requirements generation process for JEOD, the first subject reviewed was requirements generation. Requirements generation guidance existed in several areas. The four main areas reviewed were product design, systems engineering, DOD, and commercial guidance.

Product design laid out how to generate requirements to support development of a product. As this was the most straightforward approach to requirements, it was reviewed first to determine common concepts that could apply to the JEOD requirements process. The next area reviewed was the role of requirements generation in systems engineering. There was extensive guidance on requirements in the systems engineering domain and several approaches were noted as concepts to use in the JEOD requirements process. Guidance from the DOD was then reviewed as JEOD was part of DOD and mandated to use certain DOD guidance. Finally, commercial industry guidance was reviewed as commercial industry operates very differently and normally faster than DOD. As one of the goals for the new JEOD requirements generation process was to decrease the time it takes to generate requirements, this was a key component of the thesis.

1. Requirements Generation in Product Design

The first area looked at was product design. In product design, the first step of the process was to identify customer needs (Ulrich and Eppinger 2016). In the process of defining the customer needs, there were several goals: ensure that product development is customer focused, identify any hidden needs in addition to those stated by the customer, provide justification for the needs included in development, create a database of the needs, verify that no needs are forgotten, and develop a shared understanding amongst all stakeholder (Ulrich and Eppinger 2016). Ulrich made a distinction between needs and specifications (requirements). He said that, “needs are largely independent of any particular product while specifications depend on the concept selected” (Ulrich and Eppinger 2016, 75). He also stated that it is important to identify latent needs or those needs that a customer may not realize they have, however, if not met, the product will not satisfy the customer.

According to Ulrich's process, customer needs were turned into specifications which were used to develop and test the product. In order to gather customer needs, Ulrich recommended the following steps: gather needs from customers, analyze the needs, organize the needs by type, establish priority, and study the results. The methods he recommended for gathering the raw data from customers were interviews, focus groups, and observing how the product is used.

Crawley, Cameron, and Selva proposed a similar strategy where they looked at the specifications as goals as shown in Figure 3 (Crawley, Cameron, and Selva 2016).

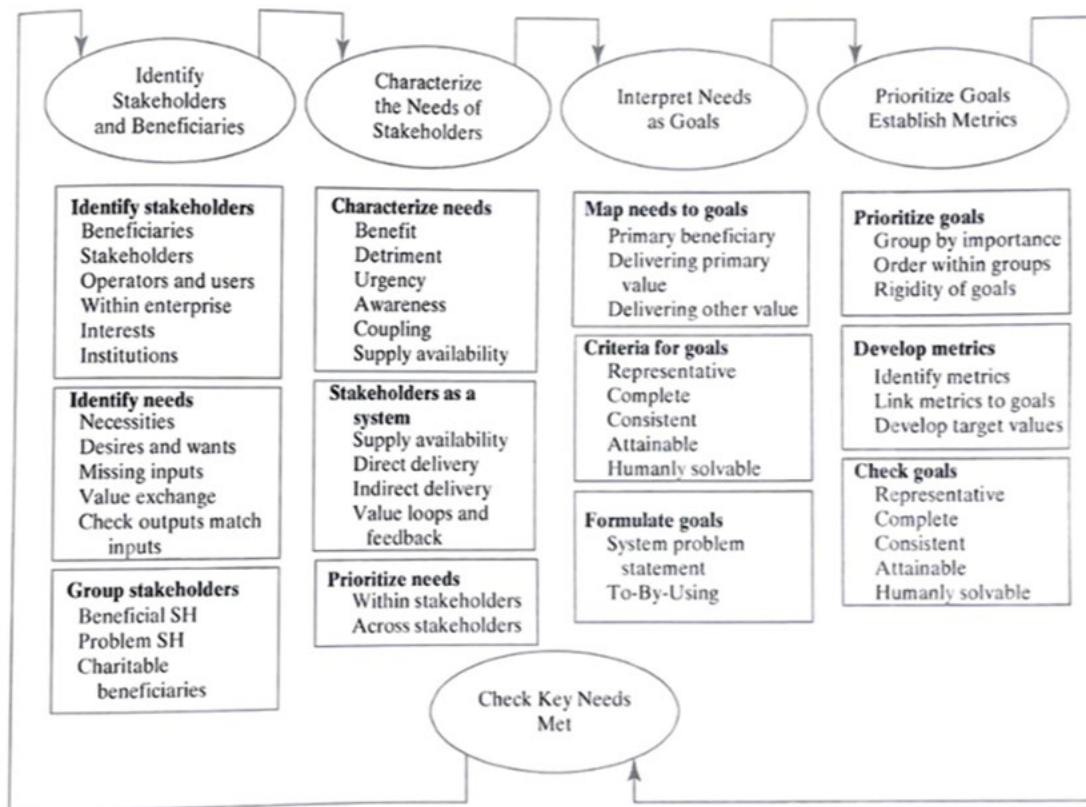


FIGURE 11.1 Needs-to-goals framework, working from the identification of stakeholder needs through to prioritized goals.

Figure 3. Needs to Goals Framework. Source: Crawley, Cameron, and Selva (2016).

Similar to Ulrich, Crawley took user needs and prioritized them. He added additional steps of identifying the stakeholders and characterizing the needs. He also set up criteria and metrics for the goals with a check that they were representative of the needs, complete, consistent with the needs, able to be attained, and solvable.

Each of these references provided guidance on how to take user needs and turn them into requirements, but they did not show how user needs and requirements fit into the bigger picture of systems engineering.

2. Role of Requirements Generation in Systems Engineering

The “International Council on Systems Engineering (INCOSE) defined systems engineering as an interdisciplinary approach and means to enable the realization of successful systems” (Walden et al. 2015, 11). INCOSE went on to say that systems engineering “focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal” (Walden et al. 2015 11). In accordance with this definition and similar to the processes in product engineering, user needs and requirements occur early in the systems engineering process.

There were several different process models identified that can be used in systems engineering. Examples were the Waterfall, Spiral, and Vee (Blanchard and Fabrycky 2011). Each of these followed a similar concept where the process starts with user needs and requirements and proceeds to design, implement, and test. Each process took a unique path to get from the starting point to the ending point. In each of these processes, requirements generation was considered a step in the process.

INCOSE further broke down the requirements generation into stakeholder needs and requirements definition process, and system requirement definition process (Walden et al. 2015). The steps derived from INCOSE for these two processes were shown in Table 1.

Table 1. INCOSE Requirements Steps. Adapted from Walden et al. (2015).

Stakeholder Needs and Stakeholder Requirements Process
1 - Identify Stakeholders
2 - Identify enabling systems or processes
3 - Gather stakeholder needs
4 - Prioritize stakeholder needs
5 - Develop operational scenarios
6 – Define interactions of system
7 – Identify constraints
8 – Develop stakeholder requirements
9 – Define measures of effectiveness (MOEs) and measures of suitability (MOSs)
10 – Analyze requirements
11 – Negotiate modifications for unachievable requirements
12 – Confirm changes with stakeholders
13 – Record requirements in a database
System Requirements Process
1 – Generate plan for defining system requirements
2 – Establish system boundary and determine interaction with external systems
3 – Identify and define the required system functions
4 – Identify constraints on system from stakeholder requirements or organizational limitations
5 – Identify critical characteristics
6 – Identify technical risks
7 – Specify system requirements. Establish hierarchy. Capture rational for each requirement.
8 – Analyze requirements
9 – Present requirements to stakeholders
10 – Negotiate modifications
11 – Define verification criteria such as measures of performance (MOPs) and technical performance measures (TPMs) which should trace to MOEs and MOSs
12 – Ensure stakeholders agree
13 – Establish traceability
14 – Record requirements in a database

While the two processes were similar, there were important differences. The “purpose of the stakeholder needs and requirements definition process was to define the requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment” (Walden et al. 2015, 52). In contrast, INCOSE stated that the “purpose of the system requirements definition process was to transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution

that meets the operational needs of the user” (Walden et al. 2015, 57). The difference between the two was in the perspective of the requirements. The first process generated requirements from the user’s perspective while the second generated requirements from the supplier’s perspective (Walden et al. 2015). A good example of how the two processes relate was shown in Figure 4.

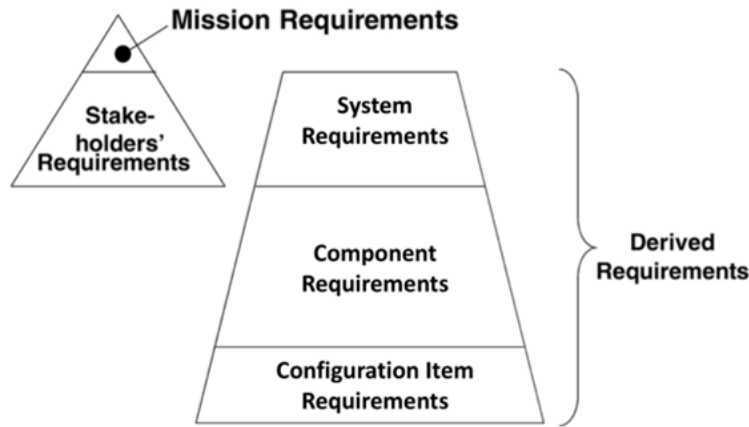
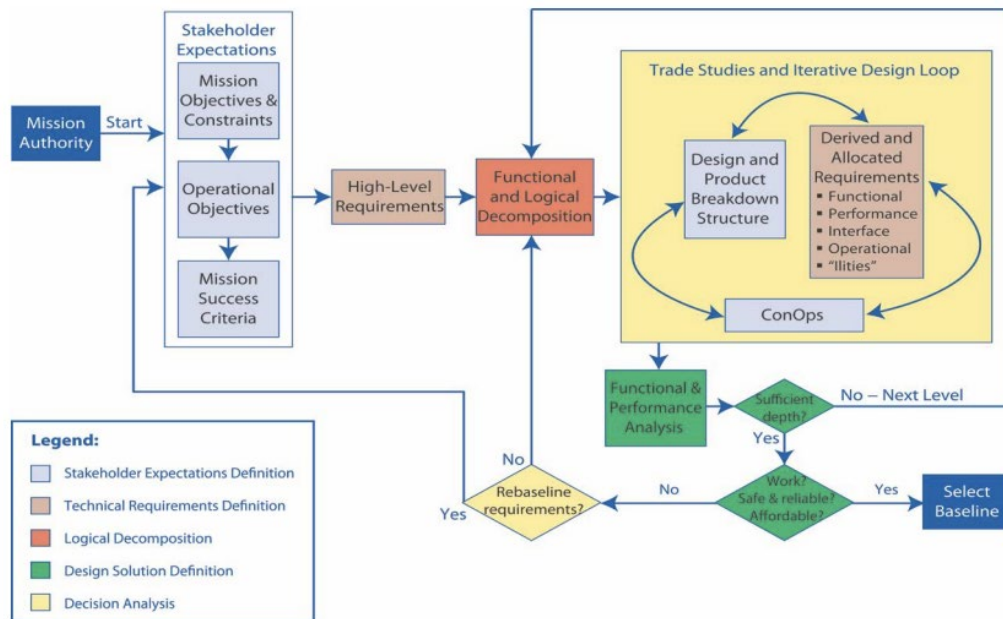


Figure 4. Requirements Pyramid. Source: Buede and Miller (2016, 148).

The stakeholder requirements from the first process were used to derive the system requirements in the second process which then got further defined for the component and configured items. The system requirements in accordance with INCOSE for the second process also had to ensure that the system could meet the stakeholder requirements.

It was important to note that this process was not serial. Rather it was an iterative process where the stakeholder needs were continuously referenced to ensure the subsequent requirements were being derived correctly. An interesting diagram was generated by the Massachusetts Institute of Technology which was shown in Figure 5.

Interrelationships Among the System Design Processes



SP-2007-6105, Figure 4.01

Figure 5. Role of CONOPS in Requirements Generation. Source: Weck (2015).

From Figure 5, it was seen that after the requirements and CONOPS have been generated the requirements are reviewed to see if they are sufficient. If yes, the process moves forward. If not, they have to be reviewed. This diagram was chosen as it pulls in the CONOPS and other elements previously discussed.

In addition to requirements generation being an iterative process, it is done at multiple stages of the life cycle (Blanchard and Fabrycky 2011). Blanchard and Fabrycky stated that during the conceptual design phase, requirements are generated at the system level. During the preliminary design phase, it is at the subsystem level, and it is at the component level during the detail design development phase. During the production and support stages, requirements were generated for modifications.

In addition to requirements being generated at various stages of the system life cycle, they are also generated at various levels of the system. From the top-level system

down to the lowest configured item. When looking at a system of systems this was even more important as each system in the system of systems had to be designed independently while still ensuring integration into the overall system of systems. The dual Vee model shown in Figure 6 was particularly useful for demonstrating this.

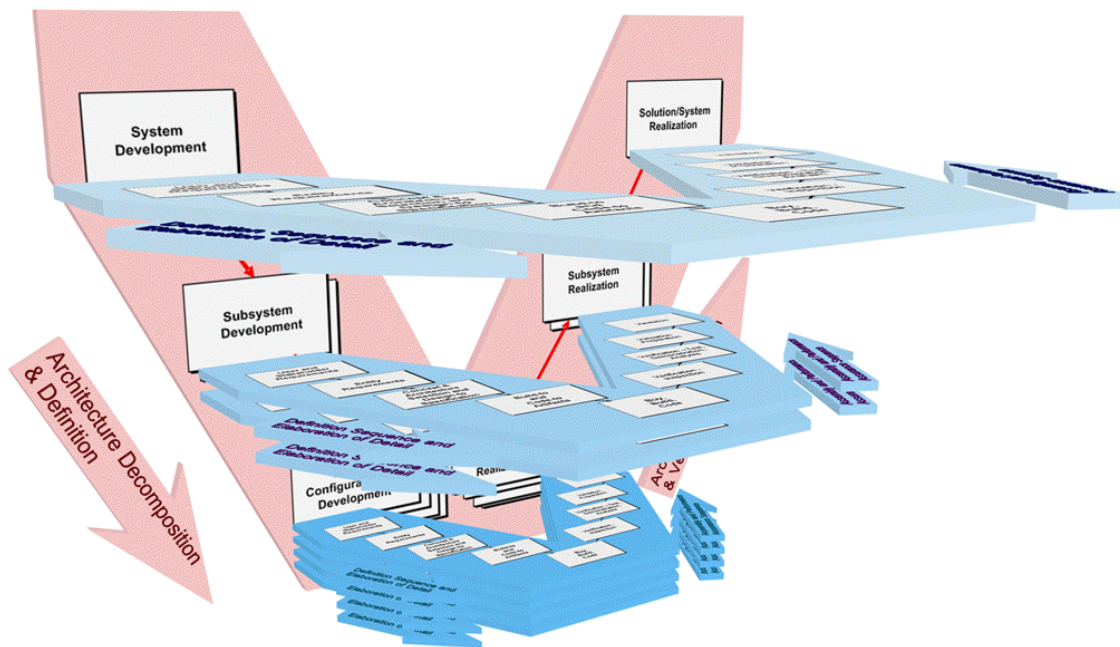


Figure 6. Dual Vee Model. Source: Mooz, Hal, and Forsberg (2006).

On the vertical axis was the overall system. Moving up and down the vertical V, the system was developed and then validated. On each of the horizontal Vs, each of the subcomponents of the system, or systems in the systems of systems also goes through the same development and validation process. It must be noted that the overall system validation could not be done until the entire system was developed at the top right of the V. Verification of each of the subsystems or systems in a system of systems could be done sooner.

Looking at the right-hand side of the V, once the requirements are generated, the next step is to analyze them. INCOSE described attributes of good requirements to be, “necessary, implementation independent, unambiguous, complete, singular, achievable,

verifiable, and confirming” (Walden et al. 2015, 61). INCOSE recommended that they trace to a parent, source, interface definition, peer requirements, verification method, priority, criticality, risk, owner, rational, applicability, and type. The *INCOSE Guide to Writing Requirements* went into even more detail on this subject (INCOSE 2012). *ISO29148* also reiterated these attributes of good requirements (ISO/IEC/IEEE 29148:2011E 2018).

While these steps helped determine if good requirements were written, they did not look at if all the necessary requirements have been generated. *ISO29148* listed several types of attributes that it said should be considered in order to determine if all necessary requirements were generated. These were shown in Figure 7.

Types of System Requirement	Description
Functional Requirements	Describe qualitatively the system functions or tasks to be performed in operation.
Performance Requirements	Define quantitatively the extent, or how well and under what conditions a function or task is to be performed (e.g. rates, velocities). These are quantitative requirements of system performance and are verifiable individually. Note that there may be more than one performance requirement associated with a single function, functional requirement, or task.
Usability Requirements	Define the quality of system use (e.g. measurable effectiveness, efficiency, and satisfaction criteria).
Interface Requirements	Define how the system is required to interact or to exchange material, energy, or information with external systems (external interface), or how system elements within the system, including human elements, interact with each other (internal interface). Interface requirements include physical connections (physical interfaces) with external systems or internal system elements supporting interactions or exchanges.
Operational Requirements	Define the operational conditions or properties that are required for the system to operate or exist. This type of requirement includes: human factors, ergonomics, availability, maintainability, reliability, and security.
Modes and/or States Requirements	Define the various operational modes of the system in use and events conducting to transitions of modes.
Adaptability Requirements	Define potential extension, growth, or scalability during the life of the system.
Physical Constraints	Define constraints on weight, volume, and dimension applicable to the system elements that compose the system.
Design Constraints	Define the limits on the options that are available to a designer of a solution by imposing immovable boundaries and limits (e.g., the system shall incorporate a legacy or provided system element, or certain data shall be maintained in an online repository).
Environmental Conditions	Define the environmental conditions to be encountered by the system in its different operational modes. This should address the natural environment (e.g. wind, rain, temperature, fauna, salt, dust, radiation, etc.), induced and/or self-induced environmental effects (e.g. motion, shock, noise, electromagnetism, thermal, etc.), and threats to societal environment (e.g. legal, political, economic, social, business, etc.).
Logistical Requirements	Define the logistical conditions needed by the continuous utilization of the system. These requirements include sustainment (provision of facilities, level support, support personnel, spare parts, training, technical documentation, etc.), packaging, handling, shipping, transportation.
Policies and Regulations	Define relevant and applicable organizational policies or regulatory requirements that could affect the operation or performance of the system (e.g. labor policies, reports to regulatory agency, health or safety criteria, etc.).
Cost and Schedule Constraints	Define, for example, the cost of a single exemplar of the system, the expected delivery date of the first exemplar, etc.

Figure 7. Types of Requirements. Source: ISO/IEC/IEEE 29148:2011E (2018).

This tied back to the guidance in INCOSE that the entire set of requirements should be looked at as a whole to ensure they were complete, consistent, feasible, and bounded. This was important as the primary consideration for choosing a system is “how well it addresses the functional need for which it was developed” (Reese 2018, 19). Reese states that “testing a system in accordance with its design specification may not reveal whether

(or well) the system can achieve its overall mission” (Reese 2018, 19). Reese quoted an excerpt from Stevens that stated:

Ideally, a system is completely defined by a set of specifications in such a way that if the system is tested and found to comply with all specifications, this assures the system can accomplish its assigned mission. In actual practice, however, each specified characteristic represents a compromise ... furthermore, some critical aspects of system performance can be overlooked in developing the breakdown into specific characteristics. The result is that the systems may often fully comply with their specifications and still prove deficient in performing their assigned missions, or alternately, the system may fail one or more specification requirements, yet still perform the mission perfectly satisfactorily. (Stevens 1979, 18)

Reese proposed that the “functional requirements formalize the users need while MOEs provide a quantitative means to evaluate the accomplishment of this need through the achievement of mission objectives” (Reese 2018, 19). He stated that the difficulty with MOEs lies in the validation. While MOEs can be developed early in the requirements generation process, they cannot be validated until operational testing at the end of the process (Reese 2018). This was shown in Figure 8.

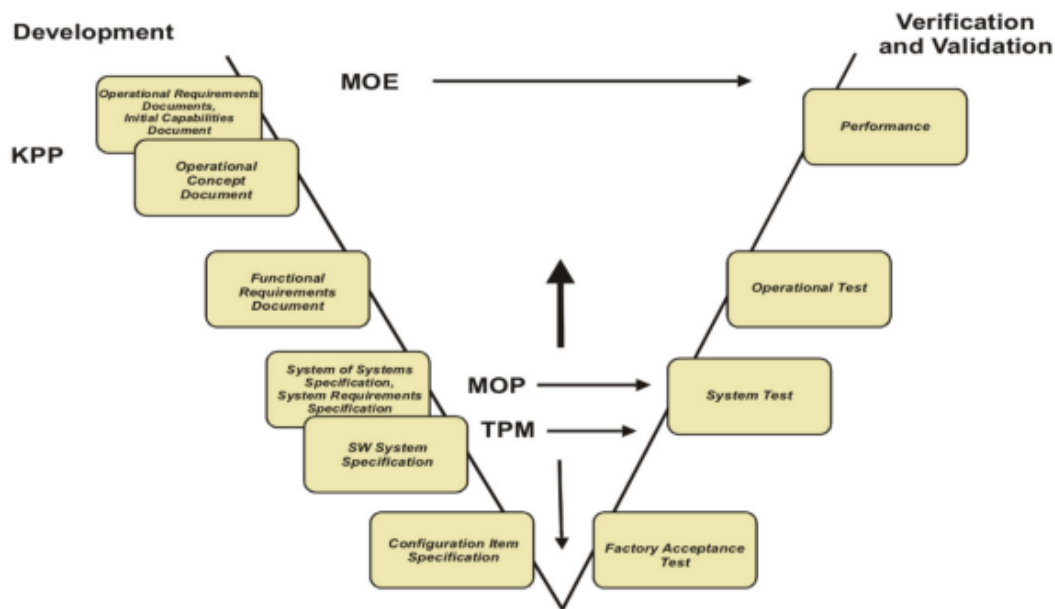


Figure 8. Systems Engineering V-Model. Source: Roedler and Jones (2005).

This makes it difficult to determine if the MOEs are well written and achievable early in the requirements process. *ISO29148* discussed that requirements should be both validated and verified. It defined “validation as the confirmation through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled,” (Walden et al. 2015, 266) or the right system has been built. While verification is the “confirmation through the provision of objective evidence, that the specified requirements have been fulfilled,” (Walden et al. 2015, 266) or the system has been built right.

ISO29148 recommended that verification be done by comparing the requirements to the attributes of good requirements. For validation, *ISO29148* recommended that stakeholder reviews, prototyping, modeling and simulation, or conceptual modeling be used.

3. Commercial Guidance

In addition to standard SE guidance, commercial guidance for generating requirements was also studied. As requirements generation for production was already presented, this section focused on requirements development for agile and software systems.

Software development had the same issues with requirements development as material systems.

The hardest single part of building a software system is deciding precisely what to build. No other part of the conceptual work is as difficult as establishing the detailed technical requirements, including all the interfaces to people, to machine, and to other software systems. No part of the work so cripples the resulting system if done wrong. No other part is more difficult to rectify later. (Brooks 1986)

Much of the guidance on software requirements generation was similar to work already discussed. It involved identifying a problem, generating user needs, assessing them, developing a solution, and verifying and validating it. One method proposed was MEASUR, which stood for Method for Eliciting, Analyzing and Specifying User’ Requirements (Sharma 2016). One of the interesting points that Sharma looked at was

subjectivity. In addition to identifying the stakeholders, which is one of the first steps in other requirements generation processes, Sharma also proposed identifying the stakeholders' motivations and biases. When mapping the physical model of the system to include its universe and stakeholders, Sharma proposed including the motivations of those stakeholders. Sharma developed schema of statements to capture the stakeholders, what they required, why, and under what conditions. For software engineering this method was useful to show how the requirements could change based on changing conditions.

Due to the long timeline that often exists between requirements generation and product delivery in traditional systems engineering, by the time the product is delivered the user needs may have changed. Agile development is used to try to address this issue. Agile development had the following principles: dedicated resources for the life of the project, collaboration to develop user stories versus the system shall requirements, brief team meetings, frequent feedback, and specifications with details of a user story.

Agile project requirements generation used epics and user stories to create scenarios and tasks that the software must do (Kitowska 2021). An example was shown in Figure 9.

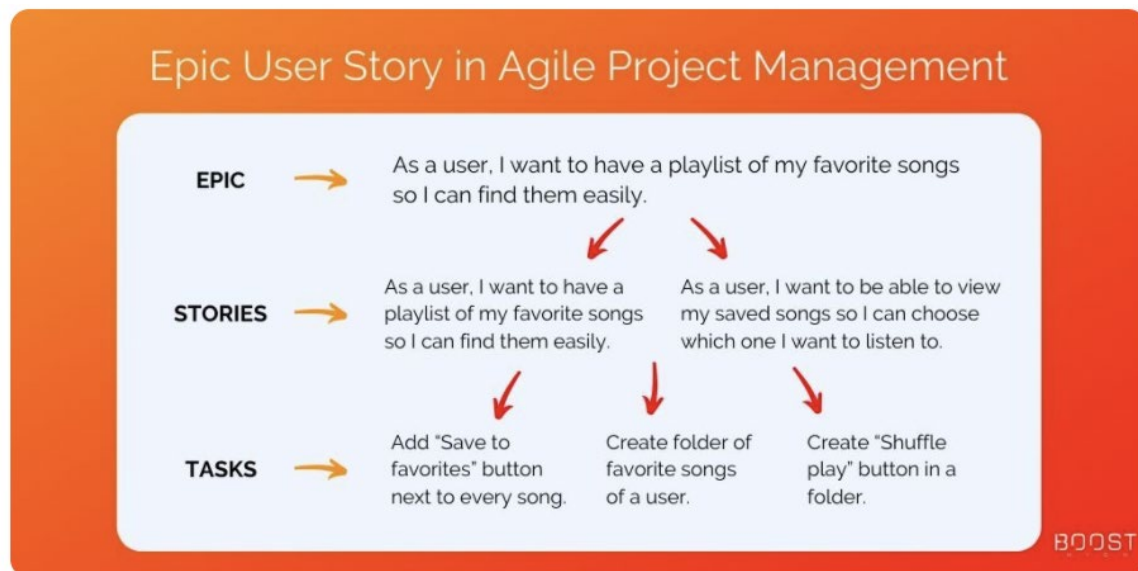


Figure 9. Example of an Epic Story. Source: Kitowska (2022).

This was similar to having a user need and using it to generate requirements. The difference was that it considered alternate scenarios and proposed solutions. The goal of the user story was to focus on the viewpoint of the user of the system, define the requirement in language the user would understand, understand the true reason for the requirement, and define the high-level requirement early without going into too much detail early in the process (Agile Business Consortium 2022). According to the *DSDM Agile Project Framework Handbook*, user stories were often composed on three elements deemed the three C's: Card, Conversation, and Confirmation. According to the handbook, on the front of the card is the conversation which includes an identifier, title, and statement in the form of "As a _ I need _, so that _." This signifies who the stakeholder is, what effect they want the requirement to have, and what they will get from it. The back of the card contains the confirmation in terms of acceptance criteria that will be used to define that the user story works as required. Like traditional SE requirements generation agile requirements development expected requirements to evolve and emerge throughout the effort.

4. DOD Specific Guidance

In order to get requirements generation guidance specific to the DOD, several documents were reviewed. The first was the *Defense Acquisition Handbook* (DAG). The *DAG* was designed to provide the DOD acquisition workforce with best practices that should be followed for acquisition of DOD systems (DAG 2022). As such it followed the DOD acquisition process model. Like INCOSE and other SE guidance, the *DAG* stated that the stakeholder requirements definition process needs to be followed so that the stakeholder requirements are feasible and balanced. It noted that failure to follow this step could lead to significant requirements creep, rework cost growth, and schedule slip. The *DAG* recommended the following steps in order to avoid these pitfalls.

- 1) Generate stakeholder objectives. What the system will accomplish and how well (MOEs).
- 2) Define the requirements. Include the constraints, relevant environment, threats, scenarios, and unidentified requirements.

- 3) Analyze the requirements. Verify the requirements, resolve discrepancies, and produce a traceability matrix.

The steps recommended by the *DAG* aligned with the SE guidance previously presented. The scenarios were also similar to the user stories in agile projects.

The *DAG* also discussed the purpose of an analysis of alternatives (AoA) which was to compare the, “operational effectiveness, suitability, and life-cycle cost of alternatives that satisfy the established capability needs” (DAG 2021, 2.3). The *DAG* stated that the AoA should, “examine potential materiel solutions with the goal of identifying the most promising solution” (DAG 2021, 2.3). It went on to say that the AoA defined the trade space across cost, schedule, and performance for each capability gap in the Initial Capabilities Document (ICD). Therefore, the AoA was performed after the ICD was developed. Items which the *DAG* listed as included in the AoA were scenarios, threats, environment, timeframe, mission tasks, MOEs, and MOPs. The *DAG* stated that the results from the AoA were to be consistent with the Capability Development Document (CDD). According to the *DAG* the inputs to Milestone A were an ICD and validated online life cycle threat (VOLT) report while the outputs were the AoA report and CDD.

Since JEOD is a joint program, requirements documents have to be validated through JCIDS. JCIDS focuses on capability development that is based on a concept and informed by a threat (Intellipedia 2021). According to the *JCIDS Manual* (Intellipedia 2021, A-1),

JCIDS starts with a robust capabilities-based assessment (CBA) of missions, functions, and tasks in the context of threat and environment, to identify and quantify Capability Requirements (CR). CRs are Measures of Effectiveness (MOE) in the form of mission focused task statements that are best written in “task, condition and standard” format. CRs are Service, solution, and cost agnostic, and are thought of as “what needs to be done (the metric), and to what level (the initial value).” CRs are defined as: “The ability to [perform a task (Universal Joint Task (UJT) or Service Task) Operational Activity] against/given a [Threat] in order to achieve [Effect] in a/under [Environmental Conditions] in the [Standard Timeframe].”

According to the *JCIDS Manual*, the CRs “are then compared with the existing and programmed capability solutions across the joint force to identify potential capability gaps”

(Intellipedia 2021, A-1). The *JCIDS Manual* went on to say that the content is captured in a document that includes, “traceability to the source of the CRs, the identification of capability gaps, assessment of associated risk, and timelines of capability solutions(s) needed by the warfighter” (Intellipedia 2021, A-1).

From the JCIDS CBA, it was determined if a materiel, information system (IS) , or non-materiel solution was required. Materiel solutions would go on to be covered by an ICD, while information systems were covered by an IS-ICD or software (SW) ICD, and non-materiel solutions were covered by a Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities – Policy (DOTmLPF-P) Change Recommendation (DCR). This thesis focused on the ICD and CDD.

The *JCIDS Manual* stated that the ICD would specify one or more CRs (tasks, conditions, and standard) and associated capability gaps that would result in unacceptable risk if not mitigated. The data in the ICD was similar to that referenced in SE documents for the generation of stakeholder needs and stakeholder requirements, as the data was from the user perspective. The ICD was also where the MOEs were generated and documented. The ICD defined the operational context, threat summary, CRs and gaps/overlaps, initial objective values, survivability considerations, and recommendations for solution paths. The Department of Defense Architecture Framework (DoDAF) views to be included in the ICD were AV-1, OV-1, OV-2, OV-3, OV-4, OV-5a, OV-6c, CV-2, CV-3, CV-6.

The CDD as discussed by the *JCIDS Manual* specified the requirements, in terms of system level performance attributes which included Key Performance Parameters (KPPs), Key System Attributes (KSAs), and Additional Performance Attributes (APAs) to support development of one or more increments of a materiel capability solution. The data in the CDD was similar to the system requirements definition process which derived the requirements from the supplier’s perspective and generated the technical performance measures (TPM)s.

The CDD took the information from the ICD and added to it. From the ICD the CDD leveraged the operational context, threat summary, CRs and gaps/overlaps, initial objective values, survivability considerations. Per the JCIDS manual, the following

sections were added, “executive summary, capability discussion, program summary, performance attributes (MOEs as well as TPMs), other system attributes, interoperability, spectrum, and electromagnetic environmental effects (E3) control requirements, intelligence supportability, weapon safety assurance, technology readiness, DOTmLPP-P considerations, and program cost” (Intellipedia 2021).

The CDD provided “threshold values for each performance attribute that represented the value below which performance would require reevaluation of military utility in the applicable CONOPS and/or Operational Mode Summary/Mission Profile (PMS/MP)” (Intellipedia 2021, B-C-9). The objective values were for increased performance level that would provide a significant increase in operational utility. The range between the threshold and objective value was to allow trade space during future development due to evolving technology, threats, or interoperability needs.

Similar to the SE guidance, the *JCIDS Manual* provided a section on the development of performance attributes and listed guidance for how to write them, Appendix G to Enclosure B. The manual also provided guides for the required KPPs and a guide to threat and intelligence supportability and certification. This particular guide had detailed information on how to identify critical intelligence parameters (CIPs), how to generate a VOLT report, and where to find threat data. The DoDAF views to be included in the CDD were those in the ICD as well as SV-1, SV-2, SV-7, and SV-8. There were additional views if the system was expected to be net ready. These were DIV-1, DIV-2, DIV-3, SV-4, SV-5a, SV-6, StdV-1, and StdV-2. Additional information on the DoDAF was found in the *DoDAF Version 2.02* (DoDAF 2010).

The *JCIDS Manual* specified paths for both urgent and deliberate documents, but this thesis only focused on the deliberate process which was shown in Figure 10.

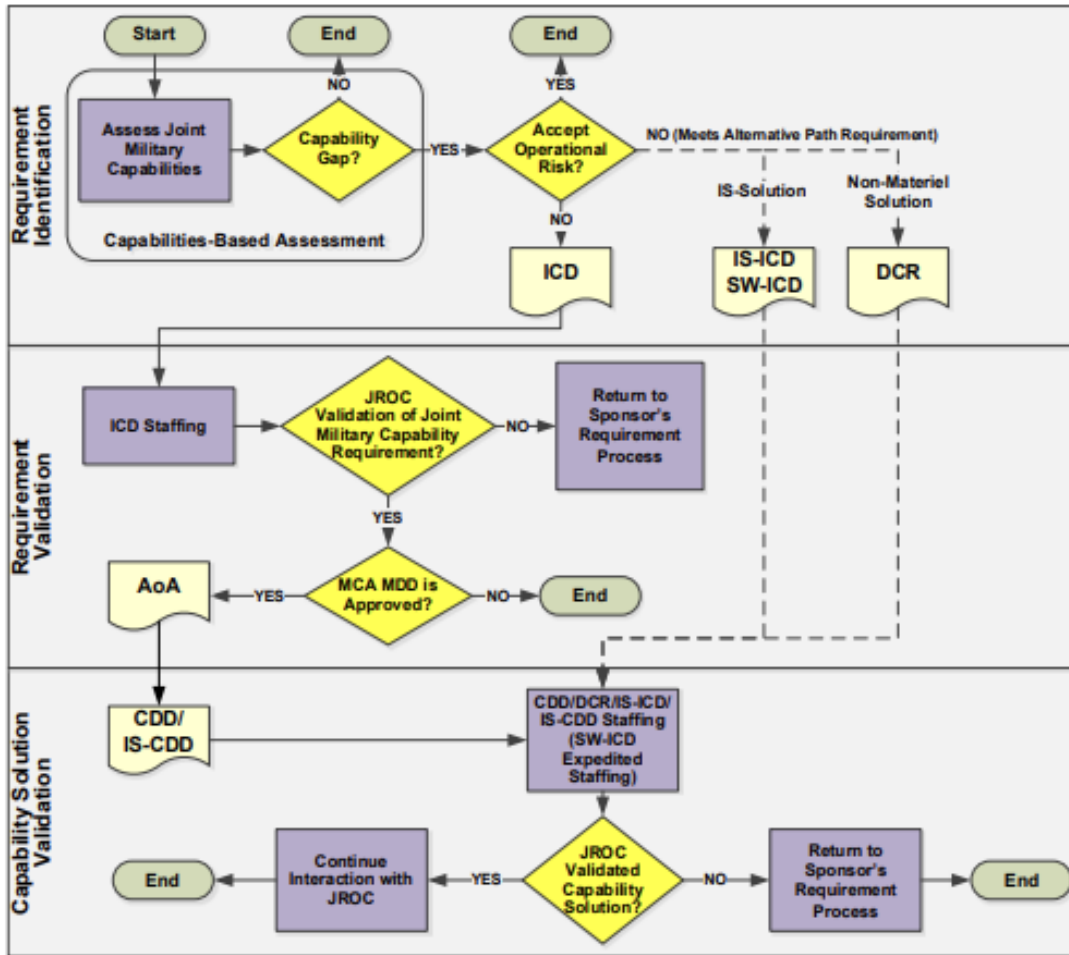


Figure 10. JCIDS Process Overview. Source: Intellipedia (2021).

Following generation of the ICD, the *JCIDS Manual* stated that an AoA or other assessment would be performed which would allow a decision to be made on how to obtain the solution to the capability gap. The results of the AoA could lead to a CDD, a DCR, multiple CDDs or DCRs, or even a CDD with multiple annexes as shown in Figure 11.

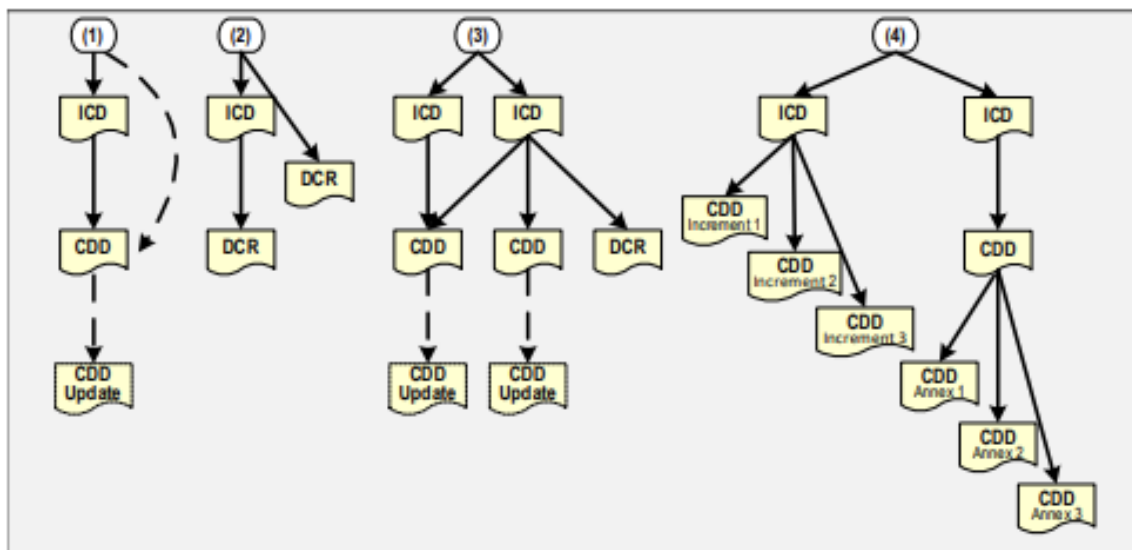


Figure 11. JCIDS Document Sequences. Source: Intellipedia (2021).

The path chosen would be based on the best approach to satisfy the CR and eliminate or mitigate the capability gap. The JCIDS manual provided specific guidance in regard to Families of Systems (FoS) and System of Systems (SoS).

The *JCIDS Manual* defined a FoS as, “similar interdependent capabilities which were provided through different approaches to achieve similar or complimentary effects” (Intellipedia 2021, GL-17). According to JCIDs, when a FoS was proposed, there had to be a base CDD with incremental annexes that followed it or annexes that are submitted at the same time as the base CDD. If incremental annexes were planned, they had to be addressed in the CDD. Each annex could provide new requirements, but the system developed by each annex still had to adhere to all the requirements set forth in the base CDD.

The *JCIDS Manual* defined a SoS as, “independent systems that were integrated to deliver a unique capability solution” (Intellipedia 2021, GL-22). In this case, JCIDS dictated that individual CDDs should be developed for each system in the SoS. Each CDD was required to address interoperability with other CDDs for systems in the SoS to ensure they remained compatible, and development was synchronized.

According to the JCIDS process, the CDD was not submitted for validation until the AoA was complete. This was to ensure that the requirements were achievable with a moderate level of risk. Once the CDD was submitted, the time until validation was defined by the JCIDS manual to be 103 days. The time for an ICD and DCR was 67 days while the time for an IS-ICD was 59 days.

While JEOD was required to use JCIDS for its requirements documents, there was also service specific requirements guidance. The United States Air Force (USAF) used Functional Requirements Documents (FRD) (AFCEC 2018). These were similar to the JCIDS CDD. Like the CDD, they included an executive summary, concept of operations, threat summary, capability discussion, program summary, requirements parameters, DOTMLPF, and life cycle assessment. The FRD added a section on analysis summary which described work already done to verify this was a needed requirement. This was similar to the JCIDS CBA. The FRD did not include survivability considerations directly, though they could be added.

The United States Marine Corps utilized the JCIDS process for development documents but also allowed for requirements memorandums when developing a single increment to meet a materiel capability gap, as long as it still complied with the guidance set forth by JCIDS (USMC 2017). The USMC also had a middle tier capability document (MTCD) that allowed for rapid development of “prototypes within an acquisition program to demonstrate new capabilities; and/or rapidly field production quantities of systems with proven technologies that required minimal development” (MARCORSYSCOM 2020, 43).

Like the USMC, the USN utilized the JCIDS documents and had a top-level requirements (TLR) document for middle tier acquisition (ASN 2018). The TLR could be used for rapid fielding or rapid prototyping as part of a middle tier acquisition (MTA) program or as a pre-cursor to a CDD for JCIDS (OPNAV 2021).

The United States Army also required the use of the JCIDS documents and had an option for middle tier acquisition (Army 2018). According to a memo from the Office of the Assistant Secretary of the Army, in middle tier acquisition efforts, rapid prototyping may occur before a validated requirement, and may even inform it (Army 2018). The memo

further stated that there must be an approved requirements documents within 6 months from the time the MTA process is started. The memo also said that the prototyping effort should begin with the most difficult requirements first to determine if the prototype project is achievable, is on the right technology path, or if the project should be cancelled.

Since JEOD is run by the Navy, the Navy process and JCIDS were used to define the new JEOD requirements process. The SE, commercial, and service specific guidance were also considered as long as they did not violate the Navy and JCIDS guidance. Existing JEOD guidance was also used to help define the new process.

5. Take-Aways from the Review of Requirements Generation Processes

One of the common themes from each of the requirements generation processes reviewed was the importance of properly identifying and tracking stakeholder needs. Each process agreed that improperly identifying stakeholder needs would lead to products that did not meet stakeholder needs. Each of the processes had their own method for how to identify and turn stakeholder needs into a product. Further analysis was needed to determine which methods would be best suited for JEOD.

In addition to the value of stakeholder needs, the review showed that determining how the stakeholders plan to use the system and why was also important. For the DOD and JEOD this would mean ensuring that the CONOPS for the system aligned with the stakeholder needs. How the system was planned to be used and why would drive the development of the system requirements.

Each of the processes also agreed that requirements needed to be written correctly to allow the system to be properly developed. While the systems engineering and DOD guidance provided details steps on how to verify that requirements were written correctly, they did not provide good guidance on how to validate the requirements or ensure that the right requirement was written.

Finally, the DOD and JCIDS guidance provided detailed steps for putting together a requirements document, but did not provide any guidance for how to generate the

requirements specific to a capability gap that needed to go in the documents. None of the guidance specifically discussed MBSE as part of requirements development.

B. MODEL-BASED SYSTEMS ENGINEERING

The previous literature review showed that the development and tracking of stakeholder needs as they related to CONOPS and requirements was important, but the sources did not prescribe a method for the tracking. One of the objectives of the thesis was to determine if MBSE would be an appropriate method for this tracking. In order to do this, the use of MBSE in requirements generation was reviewed. Additionally, MBSE was used as part of the development of a new requirement process and requirements for RLAC to determine if it was suitable tool for the generation and tracing of requirements.

1. Role in Systems Engineering Requirements Generation

INCOSE defined MBSE as, “the formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual phase and continuing throughout development and later life cycle phases.” (Walden 2015, 189). The models could be used in place of or in addition to written documents. The goal of MBSE was to increase rigor and precision, increase communication, and manage complexity in order to increase quality and productivity while reducing risk and cost (Hart 2015). The term MBSE was first used by Wymore, A. Wayne in 1993 (SEBoK 2021). While models have always been used as part of the development process, the proliferation of computers and their computational capabilities has allowed these models to become digital. Once digital, the models can be updated quickly and be interconnected in ways paper-based models cannot. Due to the increasing use of electronics and cyber components in systems, their complexity has increased which makes the utilization of MBSE an important component of the SE process.

According to studies by the Object Management Group (2009), INCOSE (2012, 2014, 2018), Jet Propulsion Lab (JPL) (2019), participants stated that they saw the most value in MBSE early in the SE process (SEBoK 2021). In particular, the respondents said that MBSE was most useful in system/subsystem architecting and during requirements analysis. This aligned with the observations in software development from Brooks that the

most critical component in development was correctly defining what to build, as it has the most impact on the success of the resulting system (Brooks 1986). If defining what to build was the most critical part of the development process, then capturing the decisions made during that definition would be the most important part of the MBSE effort. This thesis focused on the use of MBSE during the decision-making process to go from stakeholder needs to system requirement.

2. MBSE Tools

There have been multiple MBSE software programs developed that could be used during the requirements generation process. A few of these were IBM Rhapsody, Cameo, Innoslate, and CORE. Cameo is the most widely used in the USN but is not mandated for use. Innoslate is used by NPS as is Monterey Phoenix. As JEOD does not currently use MBSE for the requirements process, Innoslate and Monterey Phoenix were used in this thesis for MBSE work.

Innoslate is a MBSE tool that is designed to support requirements management and analysis, modeling and simulation, verification and validation, operations and support, and program management (Innoslate 2021). It also supports development of DODAF views, hierarchy charts, SysML, and Monte Carlo Simulations. For this thesis, it was used to model the current and new requirements process and analyze their timelines. It was also used to develop and analyze requirements for RLAC.

Monterey Phoenix is a high-level executable language developed by NPS to model complex behaviors (NPS 2022). It uses text-based code to model the interaction of actors, events, and constraints to identify emergent behavior. For this thesis it was used to model the actors and steps in the current requirements process to determine emergent behavior. It was also used in the RLAC analysis to model CONOPS and identify missing or overly constrained requirements.

III. GENERATION OF JOINT EXPLOSIVE ORDNANCE DISPOSAL REQUIREMENT PROCESS

The second part of this thesis and its first objective were to develop a new requirements generation process for JEOD. This chapter is organized into two sections that are highlighted in Figure 12: (1) the analysis of the current requirements generation process, and (2) a description of the new JEOD requirements generation process developed in this thesis project.

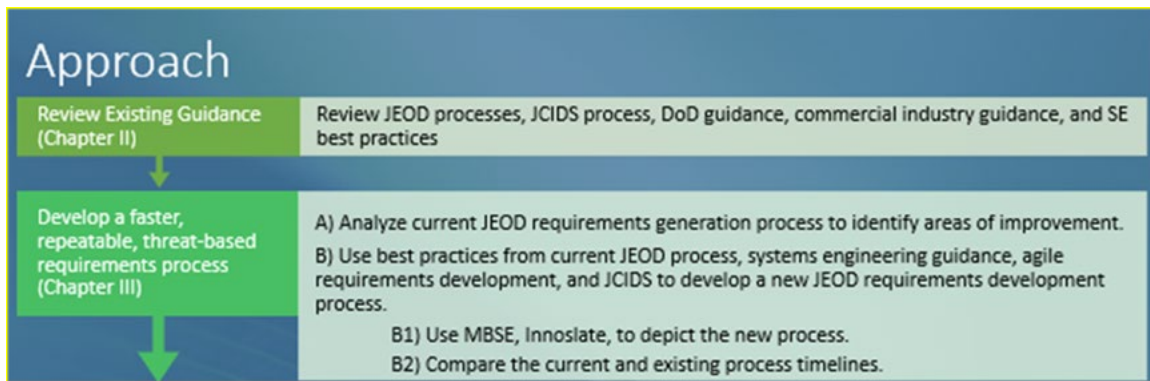


Figure 12. Chapter III Steps Taken

Section A presents the results of the SE analysis of the current JEOD processes. Its subsections follow the steps in Table 1, Stakeholder Needs and Stakeholder Requirements Process. Section B shows how the new process was developed and uses MBSE to depict it. It also shows the comparison in timelines between the current and new process. The subsections of Section B follow the steps in Table 1, System Requirements Process.

In order to generate the new requirements process, a systems engineering approach was used. A study by Swan (2017) found that, “when a system is developed using a set of requirements developed through an SE approach, it can address customer needs more completely and be produced at a greater long-term cost savings than a system that has an incomplete set of requirements necessitating additional development” (Swan 2017, v).

According to the literature review in Chapter II, there were several systems engineering models that could be used to develop a system. While each was somewhat unique, what they all had in common was that a need was translated into a product. The DOD Systems Engineering Process Model is shown in Figure 13. This model along with Table 1 were used as guides to develop the new JEOD requirements process.

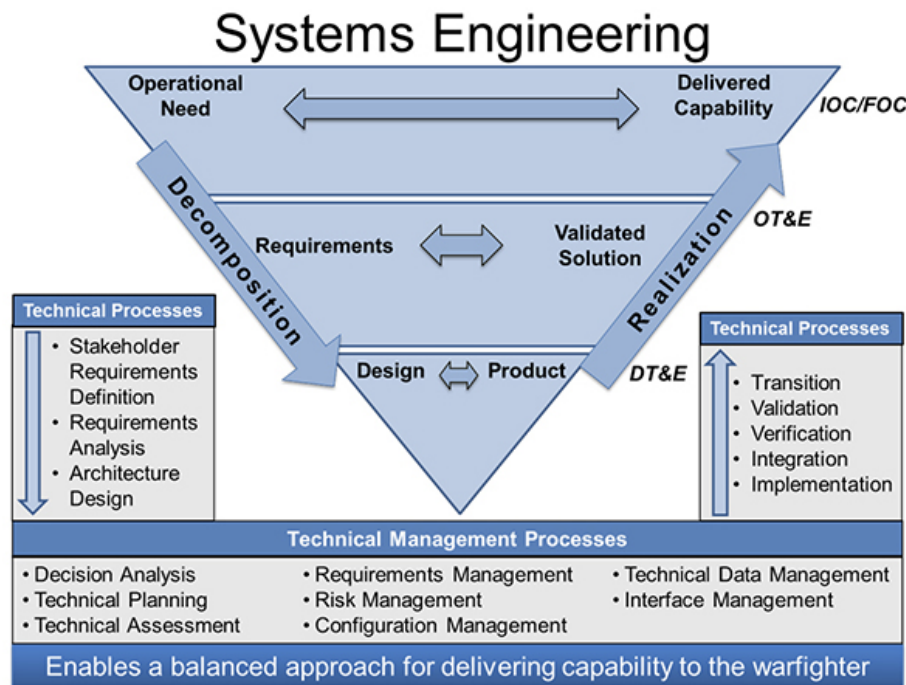


Figure 13. DOD SE Process Model of 2014. Source: DAU (2014).

The first steps that were taken to develop the process were to identify the stakeholders, identify enabling systems or processes, gather stakeholder needs, prioritize the needs, develop operational scenarios, define interactions of the system, identify constraints, and develop stakeholder requirements (Walden et al. 2015).

These steps resulted in what the process would need to do to be successful. The next step was to use the stakeholder requirements to generate the new process. The process boundary was established, new process functions were determined, and critical characteristics and risks were identified.

These steps led to the bottom of the systems engineering V in Figure 13. The results were used to develop the new process in Innoslate. The new process was compared to the current process to determine the differences in timeline to see if the new process was faster than the current process.

A. ANALYSIS OF THE EXISTING JEOD REQUIREMENTS PROCESS

1. Identifying Stakeholders

The first step which was not explicitly shown in Figure 13, but which was shown in Table 1 and was part of other product development and SE guidance, was to identify the stakeholders. The stakeholders were identified using personal knowledge of the JEOD program and substantiating it with the JEOD guidance provided in *DOD Directive 5160.62E*.

The stakeholders are shown in Table 2. If they are directly involved in the requirements generation and validation, they are listed as primary. Secondary stakeholders provide information but are not part of the approval process.

Table 2. JEOD Stakeholders

Stakeholder	Role
Sponsor – OPNAV	Primary
Gatekeeper - USN	Primary
Stakeholders - JCIDS	Primary
Functional Capabilities Board	Primary
Joint Capabilities Board	Primary
Requirements Offices – From each of the 4 services	Primary
Program Board / Action Officers	Primary
MTAB	Primary
ERB	Secondary
TTAB	Secondary
NAVSCOLEOD	Secondary
EOD Technicians – From each of the 4 services	Secondary
Program Offices – From each of the 4 services	Primary
Technology Developers – From each of the 4 services	Secondary
Industry	Secondary
JEOD T and T	Primary
ONR	Primary

Stakeholder	Role
Other DOD Technology Developers	Secondary
Academia	Secondary

In addition to Table 2, the stakeholders were mapped in Innoslate in order for them to be used as part of the MBSE for the JEOD requirements process analysis and development. When mapped in Innoslate it was seen that the stakeholders fell into four groups shown in Figure 14.

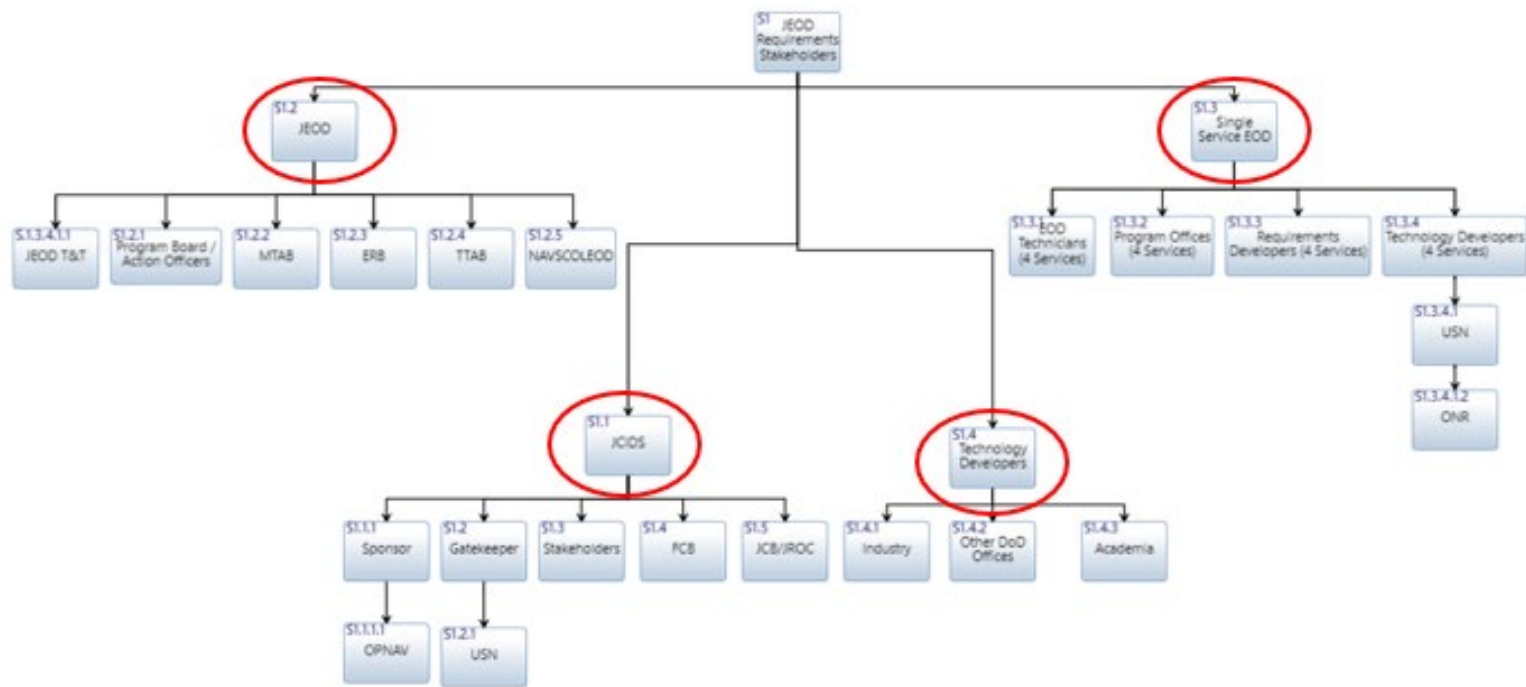


Figure 14. JEOD Stakeholders

Each of the stakeholders from Figure 14 were analyzed to determine what part they played in the process and what types of information they required from or provided to the process.

a. JEOD Stakeholders

DOD Directive 5160.62 designated the Secretary of the Navy as Single Manager for JEOD (*DOD Directive 5160.62 2021*). As such the JEOD program is resourced and managed by the Navy. There are several entities involved in supporting JEOD. Requirements for JEOD efforts are developed and funded by the Navy under Chief of Naval Operations (OPNAV).

In order to ensure that duplication does not occur and to coordinate requirements across EOD programs, representatives from each of the four services were assigned at various levels of the JEOD process. At the flag/general officers' level, the Program Board was tasked with serving "as the military services focal point and voice on EOD program requirements and making recommendations on policy and issues of common concern" (*DOD Directive 5160.62 2021*, 10). They also negotiate the annual program content and approve the plan and budget (*DOD Directive 5160.62 2021*).

The Program Board and Action Officers required requirements documents that will work to close capability gaps on the IPCL they approved. The documents must contain enough detail to allow each of their services to budget for procurement and support of the systems. The Program Board provided an approval of the requirements documents for submittal to JCIDS.

The Program Board authorized the Military Technical Acceptance Board "to approve the joint service use of all EOD specific tools, equipment, procedures, and single service EOD specific tools by military service request" (*DOD Directive 5160.62 2021*, 11). This puts the MTAB in a position to see what requirements their individual service is working as well as requirements being worked under the JEOD T and T program. They are a focal point to ensuring that requirements are consistent and non-duplicative across the EOD programs.

The inputs the MTAB requires are the approved IPCL and results from the threat process. They also require information from each of their services on items already being developed or fielded to ensure there is no duplication of effort. Their outputs are an Enclosure F SoN and CONOPS. They also provide input to the development of the requirements documents and endorse their submittal to the action officers.

The Equipment Review Board (ERB) reviews equipment and submits it to the MTAB for approval for use. The ERB requires feedback from the EOD technicians on threats, capability gaps, and the use of existing equipment. Their outputs are information from each of their services on items already being developed or fielded. They also provide input to the development of the requirements documents.

There is also a Technical Training Acceptance Board (TTAB) which “coordinates, approves, and standardizes all EOD common type individual training” and (DOD Directive 5160.62 2021, 11). The TTAB requires prototypes and information on their use to develop training plans for the NAVSCOLEOD. Their outputs are approved training for the NAVSCOLEOD.

The NAVSCOLEOD provides EOD knowledge and facilities to provide, “common-type individual EOD training to all Military Services, partner nations, and other government agencies in high-risk environments to qualify as basic EOD technicians and advanced EOD training” (DOD Directive 5160.62 2021, 8). They also “provide, as necessary or upon request, special refresher, and unique trainings on a not-to-interfere basis with basic EOD training” (DOD Directive 5160.62 2021, 9). They require approved training units and training plans. Their outputs are trained EOD technicians.

The EOD Technology and Training (EOD T and T) program role is to improve “effectiveness and economy of EOD activity throughout the DOD by eliminating duplications and overlapping of EOD technology development and training efforts” (DOD Directive 5160.62 2021, 3). Pertaining to requirements, the program ensures “attainment of state-of-the-art DOD emergency and wartime EOD capabilities by using rapid prototyping capabilities, followed by streamlined procurement procedures as much as possible” (DOD Directive 5160.62 2021, 3). Each of the single service EOD “components

may conduct EOD Research and Development programs that satisfy their unique requirements if such requirements, before initiation, are coordinated with the EOD Program Board and do not duplicate existing DOD EOD T and T program efforts” (DOD Directive 5160.62 2021, 3). This policy was designed to allow each of the single service EOD components to develop their own unique requirements without creating a duplication of effort.

In addition to the service members in the EOD T and T program, there are also other stakeholders which support the JEOD program. First, are the civilians in the EOD T and T program. Their mission is to, “provide scientific and engineering knowledge and facilities to develop, test, evaluate, and integrate equipment and technologies required to provide joint-military service EOD capabilities, including the providing of logistics support as applicable” (DOD Directive 5160.62 2021, 8). They also provide, “foreign ordnance collection, exploitation, and recovery; ordnance disassembly, intelligence analysis, and engineering; and EOD disposal and render-safe procedures development, testing, maintenance, and distribution” (DOD Directive 5160.62 2021, 8). The civilians in the EOD T and T branch work directly with the MTAB, ERB, and TTAB to perform their mission.

b. Single Service Stakeholders

Referring to Table 2 and Figure 14, since JEOD is joint and represents all four services, each of the stakeholder groups under it included stakeholders from each of the four services.

The EOD technicians are the ultimate users of the system for which requirements are being developed. They will be the ones operating and maintaining it. They require a system that allows them to perform the mission in the most effective way possible mitigating risk as much as possible. They also require training on the system in order to use it properly. They provide feedback to the requirements process that identifies the threats.

The single service project management offices roles were to manage EOD programs for each of the services they represented. They needed information from the

requirements process to determine how many systems they would buy based on the capability it provided, when the systems would be available for procurement, how much they would cost, what the sustainment plans would be, and how much they should budget for them. They also needed enough technical information to determine if the new systems would replace any of their existing systems. Their inputs to the process were IOC and FOC dates along with quantities and requirements for procurement.

The Navy program office tasked with managing JEOD efforts was SEA 05E, Explosive Ordnance Engineering (NAVSEA 2022). SEA 05E was tasked with “providing the engineering and scientific expertise, knowledge, and technical authority necessary to design, build, maintain, repair, modernize, certify, and dispose of the Navy’s ships, submarines, and associated warfare systems” (NAVSEA 2022, para. 6). In the event that requirements transition to a single service program they would be handled by that services program office.

The requirements offices of each of the services were considered as stakeholders as they would have to compare any JEOD requirements documents to their own services requirements to ensure alignment. They required copies of the requirements documents to compare them to documents used by their own services. Their inputs were information on systems in their services that required interoperability.

The last group of stakeholders under the single service stakeholders were the technology developers. They contributed information regarding the existing technology available and technology in development. The single service stakeholders’ main goal was to avoid duplication of development efforts. However, they also had their own interests in securing funding for development efforts. For the Navy, the Office of Naval Research (ONR) is the assigned technology developer. In particular, the Explosive Hazards Defeat (EHD) program works on EOD technology development efforts. They invest in basic research (budget activity 6.1), applied research (budget activity 6.2), and advanced technology development (budget activity 6.3) to support development of new capabilities for standoff defeat of explosive hazards (ONR 2022).

c. Technology Developer Stakeholders

In addition to the single service technology developers, there were other Government technology developers who also desired to secure funding and provide technology solutions. Academia was interested in securing funding to advance their research efforts and industry was interested in securing funding to develop technology and potentially transition it to production and support contracts.

d. JCIDS Stakeholders

Figure 15 showed the deliberate staffing process for CDDs and each of the players in the process.

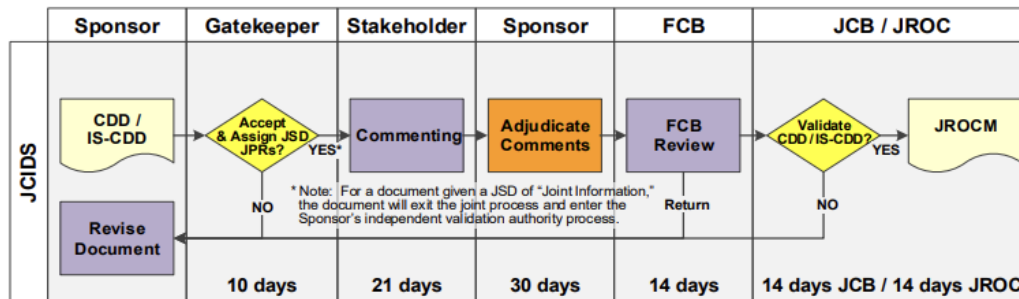


Figure 15. JCIDS Deliberate CDD Staffing (103 days). Source: Intellipedia (2021).

As the Navy is the executive manager for JEOD, OPNAV was the sponsor. The gatekeeper was also from the Navy. There were various stakeholders from each of the four services that made up the JCIDS stakeholder role. According to the *JCIDS Manual*, the stakeholders were those that are directly involved and are impacted by the efforts success or failure. Their role is to ensure that the proposed CRs are aligned with the needs of the joint force and are consistent with the National Military Strategy. The functional capabilities board (FCB) role was to review the documents, resolve any differing stakeholder views, provide a recommendation to the JCB, and ensure that the capability will provide value to the joint force and not duplicate existing efforts. The JCB or JROC

validates the CDD if it cannot be delegated down to the Sponsor. Most JEOD documents were JCB interest.

The inputs the JCIDS stakeholders required were the requirements documents from the sponsoring service along with their supporting documentation such as AoA report, DoDAF document, and VOLT report. Their outputs were validated requirements documents. Their main need was to ensure that the submitted documents were written in a manner that prevented systems from being developed and fielded that were not able to be operationally effective throughout their life cycle. They also needed to ensure that the documents did not duplicate efforts already developed or being developed by other sponsors.

2. Identifying Enabling Processes

Once the stakeholders were defined, the next step according to Table 1 was to identify the enabling processes, products, or services. These were the threat analysis process, capability gap definition process, current requirements process, and JCIDS process.

a. Threat Analyzation Process

In May of 2015, the first “Emerging Technologies and Future Threats to EOD Expo” was held to bring the EOD community with their supporting technology and intelligence communities together (Weisman 2017). The event continued to be held annually and in 2021, a threat assessment was held where, “JEOD virtually brought together over 145 participants across 51 organizations, including the intelligence community, operational EOD forces, Department of Defense and other government agencies” (NSWC IHD Public Affairs 2021). From the Public Affairs office,

Per the Commanding Officer at the time, Capt. Eric Correll, “The expo brought together the best and brightest in the field of EOD to identify and prioritize these gaps in the critical mission areas.”

The events purpose was to examine threats that EOD operators may encounter during missions. Using a variety of intelligence sources, reports and operational plans, teams worked together to identify the current top

threats across a variety of war fighting domains and EOD mission sets. These threats were then prioritized to be used as inputs for the threat Expo.

The threat Expo continued the analysis by bringing together smaller teams of technical experts to assess EOD capabilities against those threats in four consolidated mission areas: underwater, surface, buried/improvised explosive devices, and chemical, biological, radiological and nuclear munitions and weapons of mass destruction. This was the first time a threat-based assessment was layered into the normal capability-based assessment of the current state of technology. The outcome of the event was an updated capability gap list for the JEOD program to focus on future development priorities.

b. Capability Gap Definition

The capability gap list from the threat expo was used by JEOD to determine where capability gaps existed that require new solutions. Similar to the model by Hitchins in Figure 16, JEOD used the threat process to determine the issue (threat), identify problem symptoms (Threat Analysis), group problem symptoms into common themes (CBVM), model problem themes (Threat Expo), and identify differences between real and ideal world (Capability Gap).

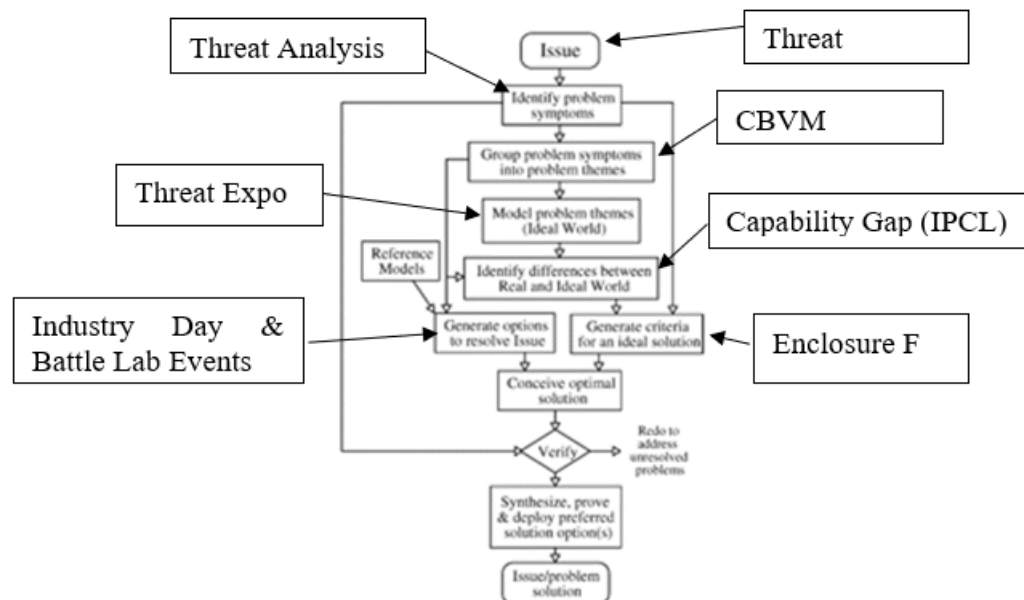


Figure 16. Systems Engineering Combined Model. Adapted from Hitchins (2007).

The CBVM process took the outputs from the threat process in the four common mission areas and compared them to the JEOD operational tasks of, “detect, locate, access, identify, diagnose, render safe/neutralize, recover, exploit, and dispose” (CJCS 2016, I-2). It then determined where capability gaps existed and defined the details of what the solution would have to do to close the gap. This was similar to the step in Figure 16 that generated criteria for an ideal solution. The resulting gaps were also prioritized in the integrated prioritized capabilities list (IPCL). Each of the gaps was looked at to propose a materiel or non-materiel solution which was informed by Industry Day and Battle Lab events. At this point, the next step according to Figure 16 was generate criteria for an ideal solution. At this point in the JEOD process the threat and capability definition process ended, and the requirements process began. Its inputs were the data from the threat process and the capability definition process. The *Department of Defense Explosive Ordnance Disposal Program Board Policy Agreement 5100.01* provided more definition (JEOD 2017).

c. Current Requirements Process

Prior to the threat and capability definition processes being used in conjunction in 2015, the outputs from the CBVM process were used to generate statement of need (SoN) documents which articulated the users perceived needs to close the gaps identified in the CBVM process. Notional concept documents were also generated by users to describe technology gaps that they saw in the field. The notional concept documents were turned into SoN documents which were forwarded to the resource sponsor OPNAV to request resourcing. If OPNAV validated the SoN document, it was assigned to the program office SEA 05E to generate a document for entry into JCIDS.

There is a JEOD ICD validated through JCIDS which documents the user’s capability requirements for the entire EOD mission set of detect, locate, access, identify, diagnose, render safe/neutralize, recover, exploit, and dispose (JEOD 05). This single ICD was used for all CDDs generated by JEOD since its validation.

Due to the lack of CDDs being generated by JEOD, the notional concept and SoN documents were transitioned to an Enclosure F document. The Enclosure F document more

closely aligned with the information required in an ICD to include work already being done and level of existing technology. The Enclosure F document was intended to provide additional detail prior to the generation of the CDD or other JCIDS documents.

Generation of the Enclosure F documents was started by OPNAV upon receipt of the IPCL approved by the program board (Shell 2021). Based on the IPCL priorities, OPNAV would work together with MTAB and EOD T and T to identify which enclosure F documents would be generated to address the gaps on the IPCL. According to the Enclosure F, the MTAB would develop the Enclosure F documents and submit them to OPNAV. Once OPNAV received and validated the Enclosure F document, they would stand up a requirement working group to generate the appropriate requirements documents, CDD, DCR, or TLR.

Each of the current JEOD processes was mapped in Innoslate to show what information they produced and what functions they performed. These were shown in Figures 17 and 18.

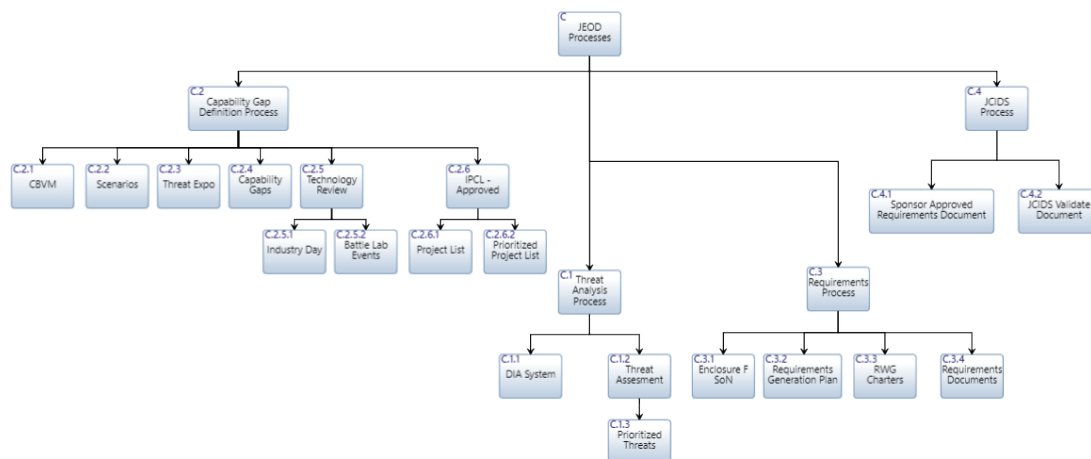


Figure 17. Current JEOD Process Asset Hierarchy Chart

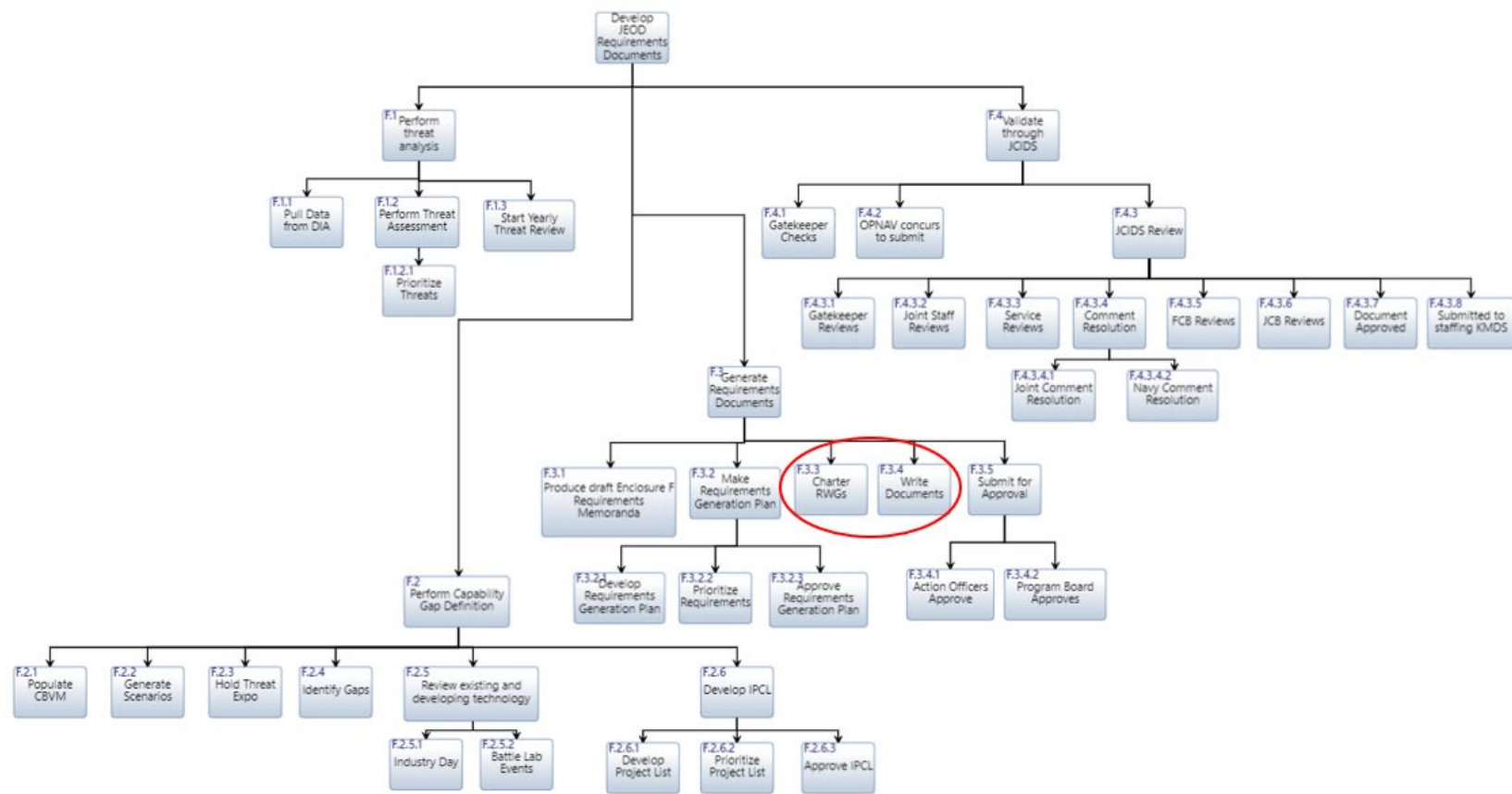


Figure 18. Current JEOD Process Hierarchy Chart

From Figure 18, under the generate requirements document's function, the Enclosure F document laid out the who, what, when, why for generating the JCIDS documents. The JCIDS guidance laid out the details of what should be in those documents. What was still undefined was the steps needed to take the data from the threat and capability processes and turn it into the detailed information in the JCIDS documents in the Charter RWGs and Write Documents Blocks. These were the functions that were the focus of the analysis.

3. Gathering Stakeholder Needs

As seen in Figures 17 and 18, JEOD already had a process to identify capability gaps. Therefore, the scope of the new requirements process started at the end of capability gap definition. Using the data gathered from the stakeholders in Figure 14 as well as what was known about the enabling processes shown in Figure 18, the stakeholder needs were developed based on personal experience as shown in Appendix B, Table 12. In addition to listing the needs, each one was defined as stated or latent. Stated needs were those required for the process to continue while latent needs were not required but contribute to the process.

4. Prioritizing Stakeholder Needs

In order to prioritize the stakeholder needs, they were analyzed and grouped using Innoslate. Figure 19 showed that the stakeholder needs fell in 6 main areas.

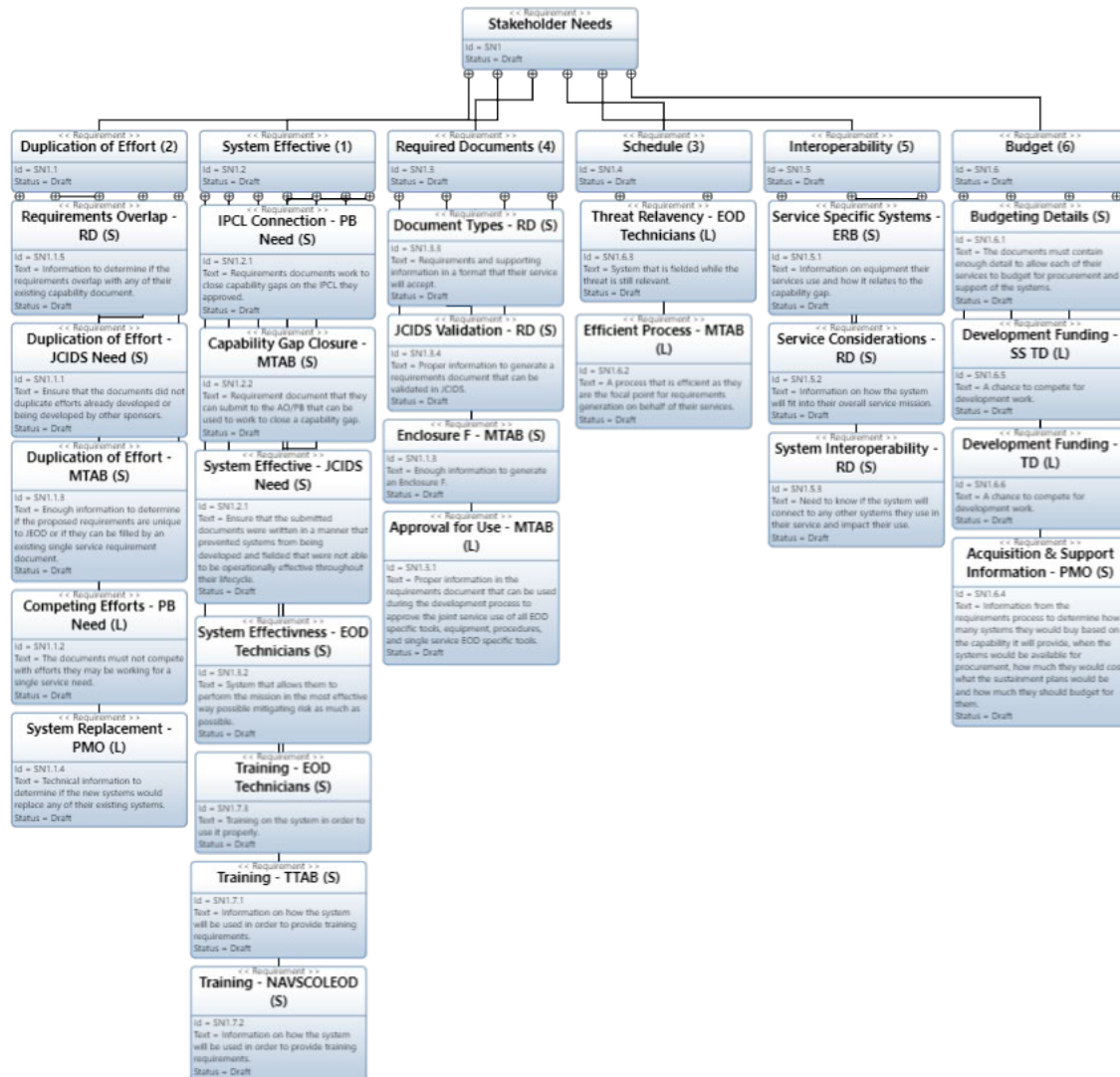


Figure 19. Stakeholder Analysis

System Effectiveness had the most stakeholder needs which was expected as the system is only useful if it performs its mission effectively. All the needs under system effectiveness were also stated needs. Due to this, the needs under system effectiveness were given the highest priority of one.

Duplication of effort was ranked second, as it also had a large number of stakeholders needs and the stakeholders would not approve the requirement if it duplicated existing efforts.

Even though required documents, interoperability, and budget had more needs than schedule, schedule was ranked third. This was due to the fact that the system would only be effective (ranked one) if it was delivered quick enough to counter the threats.

Required documents was ranked fourth as not having the required documents would stop or slow down the process. It was not ranked higher as it was possible for each of the services to take the provided information and pursue development through a single service process.

Interoperability was ranked fifth followed by budget at sixth. Interoperability overlapped in some ways with duplication of effort. Having an effective system delivered quickly was more important than having one that was interoperable with a large amount of existing equipment. Budget was not ranked higher as at this point in the process, the needs pertain to budget information in the required documents which was ranked fourth. OPNAV funds the requirements development.

Based on the above stakeholder needs analysis, an overall stakeholder need was defined as, “The JEOD requirements process needs to generate service required documents that contain the information required to budget for, develop, field, and support a system that is able to reduce or close an existing capability gap without negatively impacting existing service requirements.”

5. Developing Operational Scenarios

As the requirements development process is part of the JEOD process shown in Figure 17, the overall process was mapped out in Innoslate to show how each of the processes fit together and how the overall process was executed.

6. Defining Interactions of System

The existing JEOD threat data process, capability gap definition process, Enclosure F process, and JCIDS process were analyzed to establish the steps of the existing JEOD processes which were modeled in Innoslate. Example data was used for each step in the process and a Monte Carlo Simulation was run to establish a timeline for the current process. This was done to establish a baseline to compare the new process to.

a. Existing JEOD Process

In order to define the scope and boundaries of the new process, the existing processes were used as a guide. Each of the main areas; threat analysis process, capability gap definition, requirements generation, and JCIDS validation was represented as shown in Figure 20.

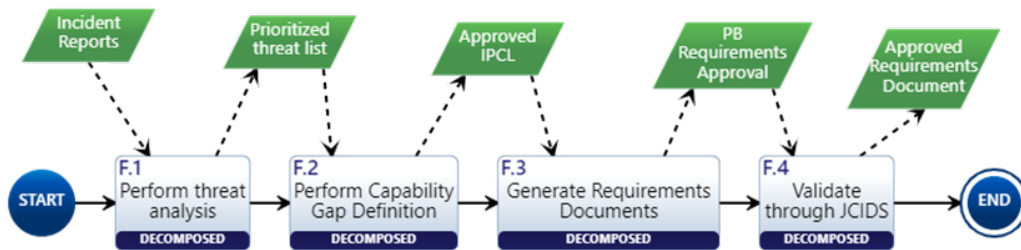


Figure 20. Existing JEOD Requirements Process

Each of the functions was decomposed in Appendix A Figures 54–57 to show the steps as currently performed in each of the processes. The JCIDS validation process was well defined and had clear inputs, outputs, and steps. The threat analysis and capability gap definition processes also had defined steps. It was noted that the threats were not carried through the capability gap definition process once they were used to generate the CBVM. While the Enclosure F guidance provided detailed steps for making a requirements generation plan and submitting it for approval, it did not provide detailed steps for writing the requirements documents. This was the area that the thesis focused on when developing the new process. It was also worth noting from Figure 20 that the process was currently performed in serial with each step occurring after conclusion of the previous one without iteration.

Once the existing JEOD requirements process was modeled, example times were associated with each step. A Monte Carlo Simulation was run to determine how long the process would take from start to end as shown in Figure 20. The mean time was found to be 1.98 years. The times for each process were shown in Table 3.

Table 3. Current JEOD Requirement Generation Timeline

Step	Time
Perform threat analysis	14 days
Perform capability gap definition	5.52 months
Generate requirements documents	1.13 years
Validate requirements documents	4.24 months

When focusing on the generate requirements documents step, the longest timeline was for writing the documents as shown in Table 4.

Table 4. Write Requirement Document Timeline

Step	Time
Produce Enclosure F Requirements Memorandum	28 days
Make requirements generation plan	4.84 months
Charter RWGs	28 days
Write documents	6 months
Submit for approval	28 days

It was noted that the above times were for writing a requirement document for one capability gap.

b. Comparison to Other Requirements Processes

The existing process was then compared to documentation on requirements development as defined by standard systems engineering guidance, DOD, JEOD, and commercial entities to establish any commonalities or differences. Each of the processes was broken down in Excel and then compared to see where there was commonality or missing steps.

When the current process was compared to the product development process from Ulrich and Eppinger the steps for requirements generation lined up as shown in Appendix

B, Table 13. As their steps were more product oriented, this format was not a good fit as it did not have enough detail in the requirements generation section.

The next process used for comparison was from Crawley, Cameron, and Selva. This approach had an initial step of identify stakeholders which was not part of the current process shown in Appendix B, Table 14. Like the product development process, the steps lined up with the current process, but there was not enough detail in the requirements generation section to develop a new process.

The INCOSE process was the most detailed in the requirements generation section. While the steps in the INCOSE process did match up with the current JEOD process, they were not in a sequential order as shown in Appendix B, Table 15. The most notable exception was that the steps for developing stakeholder needs were meant to be detailed in INCOSE but for the current JEOD process they are defined at a high level only. Like the process from Crawley, Cameron, and Selva the stakeholder identification was not done explicitly in the JEOD process. The INCOSE process did go into significant detail for the steps that lined up with writing requirements documents, so it was a good candidate for using as a guide for new process development.

The last two processes the current JEOD process was compared to where the DOD SE Model (DAU 2014) and the Agile process (Kitowska 2022). The DOD SE model had a limited number of steps as shown in Appendix B, Table 16. The Agile process also had a limited number of steps as seen in Appendix B, Table 17, but it defined the steps in a unique perspective that was not currently used in the JEOD process. The Epic user need aligned with the work done during the threat process while the stories lined up with the work done in the capability gap definition process. The cards for each story lined up with the work done during the production of the Enclosure F requirements memorandum and the creation of tasks lined up with the work done to write the requirements document.

c. Comparison to JCIDS

In addition to comparing the current JEOD process to other development processes, specific attention was paid to the JCIDS process as it was the process JEOD was required to use. Monterey Phoenix was used to model the current JEOD process and compare it to

the sections required in a CDD to see if the current process generated the required documentation for a CDD.

The first step was to determine what the major sections of a JCIDS CDD were, what type of information was required to populate them, and which stakeholders would have the information. Innoslate was used to model the connections as shown in Appendix A, Figure 56.

From Appendix A, Figure 58, it was seen that in order to write the CDD there were 13 sections that had to be generated. Per the JCIDS manual the sections are, “operational context, threat summary, capability discussion, program summary, performance attributes, other system attributes, joint interoperability, spectrum electromagnetic environmental, intelligence, weapon safety, technology readiness, DOTmLPF, and program affordability” (Intellipedia 2021). When each of these areas were reviewed to see what type of information was required to populate the sections the following were identified: CONOPS, threat data, related work, acquisition plan, and AoA report. While each of these was required to finish the CDD, the item with the most connections to CDD sections was the CONOPS followed by the related work. This was because of how the system was to be used influenced the requirements for its use. Related work helped scope the bounds of the problem defining what technology and processes were already available.

Once the JCIDS steps and required documentation were defined, the stakeholder responsible for each of the required documents was identified as shown in Table 5.

Table 5. JCIDS CDD Required Documents with Stakeholders

Required Documents for CDD	Responsible Stakeholder
CONOPS	MTAB
Threat Data	Threat SME (JEOD T and T)
Related Work	ONR
Acquisition Plan	Project Management Office
AoA	Project Management Office

It was the role of the requirements writer under OPNAV to gather all the required information and generate the overall CDD. An MP program was then written that showed each of the steps the stakeholders would need to take as ROOT functions. The data they required to complete the steps was shown in COORDINATE statements. The overall program code was shown in Appendix C, Figures 63–74. An example of the ROOT and COORDINATE functions for the threat SME was shown in Figure 21.

```

/*Threat Subject Matter Expert Actions.  Expert on threats that JSEOD faces.
They can either provide the requested data or not provide the data.*/
ROOT Threat_SME: (Analyze_Threats
                  (Provide_Threat_Data | Do_Not_Provide_Threat_Data)
                  |(Do_Not_Analyze_Threats-Do_Not_Provide_Threat_Data)
                  )
;

/*Data that they must have to complete their actions. */
COORDINATE $a: Provide_CONOPS FROM MTAB,
            $b: Analyze_Threats FROM Threat_SME
            DO ADD $a PRECEDES $b;
            OD;

COORDINATE $a: Do_Not_Provide_CONOPS FROM MTAB,
            $b: Do_Not_Analyze_Threats FROM Threat_SME
            DO ADD $a PRECEDES $b;
            OD;

```

Figure 21. Example Monterey Phoenix Code ROOT Threat SME

From Figure 21, it was seen that in order for the threat SME to analyze the threats, they had to have the CONOPS data from the MTAB. If the MTAB did not provide the CONOPS data, then the threat SME could not analyze the threats. ROOTS and COORDINATE statements similar to these were performed for the MTAB (Appendix C, Figure 64), Project Management Office (Appendix C, Figure 65), ONR (Appendix C, Figure 66), and the requirements writer (Appendix C, Figure 67–68).

Once all the actions were written into MP and tested to ensure they were working properly, a check was put into the program to mark any traces that had all the sections completed that were needed for the CDD. This allowed the resulting traces to be quickly scanned to see which ones led to a CDD being completed (Appendix C, Figure 69).

The program Model of Supply Chain with Two Cyber Threats from the MP database was used as reference code to map the likelihood and impact of the required data not being provided and the resulting CDD sections not being written (Alden and Talkington 2020). The code was modified to reference events from this program as shown in Appendix C, Figures 70–74. The risk likelihood and impact values were based on data gathered from the generation of the SRSD CDD. If the data was provided on time and was complete it was assigned a risk likelihood of 0.1 since the risk was low. If the data was provided on time but incomplete, it was assigned a likelihood of 0.5 as it led to rework. If the data was provided late but was complete it was assigned a likelihood of 0.3. This was due to the fact that it was provided but delayed the effort.

When the program was run at scope 1, it produced 9 traces which were shown in Appendix C, Figures 75–83.

Trace 1 was the only trace which resulted in the CDD being completed. All the required data was provided and the CDD was able to be written. The total risk for trace 1 was 39.8 and the breakdown for the risk in each area was shown in Table 6.

Table 6. Event Risks for MP Trace 1 CDD

Event	Likelihood	Impact	Risk Score
Provide_Related_Work_Data	0.1	5	0.5
Analyze_Threats	0.1	10	1
Provide_Acquisition_Data	0.5	10	5
Provide_Related_Work_Data	0.1	5	0.5
Write_Operational_Context	0.5	10	5
Write_Threat_Summary	0.1	10	1
Write_Capability_Discussion	0.3	10	3
Write_Program_Summary	0.5	10	5
Write_Performance_Attributes	0.3	7	2.1
Write_Other_System_Attributes	0.3	7	2.1
Write_Joint_Interoperability	0.3	10	3
Write_Spectrum_Electromagnetic_Environmental	0.1	3	0.3
Write_Intelligence	0.1	5	0.5
Write_Weapon_Safety	0.1	3	0.3
Write_Technology_Readiness	0.5	10	5
Write_DOTmLPF	0.1	5	0.5
Write_Program_Affordability	0.5	10	5

From Table 6, it was seen that the highest risk was in the areas of acquisition data, operational context, program summary, technology readiness, and program affordability. This was because both their risk likelihood and impact led to a higher risk score. The areas of analyze threats and threat summary also had high impacts but had low risk probabilities due to the robust threat assessment process JEOD utilized. The remaining areas had lower risks and impacts, but it was noted that capability discussion, performance attributes, and other attributes also had elevated risk likelihood.

The remaining traces resulted in the CDD not being completed. The probabilities for each of the traces along with the reason the CDD was not completed were shown in Table 7.

Table 7. CDD Completion Trace Probability

Trace #	Probability	Trace Risk	Result
1	0.0417	39.8	All items provided. CDD completed.
2	0.0417	34.8	AoA Report not provided. Technology Readiness not written. CDD not completed.
3	0.0417	24.8	Acquisition Plan not provided. Program Summary and Program Affordability not written. CDD not completed.
4	0.0417	19.8	Acquisition Plan and AoA not provided. Program Summary, Program Affordability, and Technology Readiness not written. CDD not completed.
5	0.0417	38.8	Threat Summary not provided. CDD not completed.
6	0.0417	33.8	Threat Summary and AoA Report not provided. CDD not completed.
7	0.0417	23.8	Threat Summary and Acquisition Plan not provided. CDD not completed.
8	0.0417	18.8	Threat Summary, Acquisition Plan, and AoA not provided. CDD not completed.
9	0.667	N/A	CONOPS not provided. Nothing written. CDD not completed.

From Table 7 it was seen that the threat summary, acquisition plan, and AoA Report are all important to completing the CDD. However, it was the CONOPS that were the most crucial. The greatest probability trace was Trace 9 where the CONOPS were not provided and the CDD could not be written. Ensuring that CONOPS are complete and provided on time was the item noted to have the most impact on CDD completion and should be addressed in the new process.

It was noted from Appendix C, Figures 75–83, that when the threat summary, acquisition plan, and AoA Report were not provided, the performance attributes and other system attributes were still written. This implied a disconnect on how that data is currently gathered as those parameters should depend on results from the threat summary, acquisition plan, and AOA report. The new process should ensure that the parameter development is linked to these items.

7. Identifying Constraints

Based on the analysis of the current JEOD process, there were several constraints which applied to the current process. They were shown in Appendix B, Table 18. The constraints were labeled as hard if they were required in the new process or soft if there was room for adjustment. In general, soft constraints were constraints that JEOD could control and change. The soft requirements were looked at as chances for change to improve the new process. In particular, it was seen that the MTAB was a pivotal stakeholder and had several responsibilities that the process was dependent on such as the Enclosure F, CONOPS, assisting with requirements development, representing the needs of the JEOD Technicians, and representing the requirements developers, program offices, and technology developers in their services. In order to alleviate some of the MTAB responsibilities, a requirements writer was hired by OPNAV to lead the writing of JCIDS documents.

The next group of constraints was the required documents. Due to the required use of JCIDS, a CDD, AoA, and DoDAF were required. These were all hard constraints and related to the resource constraints as they had to be generated by the requirements writer, with the exception of the AoA which was written by the Program Office.

The fact that JEOD was joint also added several constraints. These came in the form of multiple approvers and significant chance for overlap and interoperability considerations. These were all items that would slow the process down. Gathering information was the main challenge as the MTAB was identified as responsible for coordinating these activities. The IPCL link was also joint but a positive as it ensured that the requirements documents being written were based on a capability gap that all the services agreed to.

Lastly, timing was identified as a constraint. Both the threat analysis and budget process were on yearly cycles. The budget process was a hard constraint that could not be moved, and the development of any documents would have the most impact if it lined up with the budget process to allow for the quickest possible procurement. However, it takes

time to run the threat and resulting capability gap analysis before the requirements can be started.

8. Developing Stakeholder Requirements

Stakeholder requirements for the new process were developed by using information from the constraints, the stakeholder needs, and the analysis done on enabling systems. The hard constraints provided requirements that were required in the new process. The soft constraints were included as requirements if they added value. Information from the analysis that was noted as a negative in the existing process was turned into stakeholder requirements as applicable.

Before the stakeholder requirements were grouped and analyzed, they were compared to Figure 7 to see if any areas were not considered. Each of the areas contained several requirements except for Modes/States, Physical Constraints, and Logistical Considerations. For Modes/States it was determined that a requirement should be added to for the process to be able to handle both urgent and deliberate documents similar to the JCIDS process. For Logistical Considerations, a requirement was added that stated that the process should be able to be performed by a requirements writer. Currently there is only one requirements writer. While this could be considered a constraint as well, it was not added to the constraints to not limit the process. Once the requirements were compared to Figure 7, they were mapped in Innoslate as shown in Appendix A, Figure 59.

9. Developing Measures of Effectiveness (MOEs) and Measures of Suitability (MOSs)

From the Stakeholder Requirements, it was seen that the major functions of the process were to provide the steps to go from IPCL approval to JCIDS submittal, work to close a capability gap on the IPCL, and consider the impact to existing service work. This was similar to the overall stakeholder needs statements of, “The JEOD requirements process needs to generate service required documents that contain the information required to budget for, develop, field, and support a system that is able to reduce or close an existing capability gap without negatively impacting existing service requirements.”

Therefore, the first MOE was, the process shall be able to produce the information and documentation that will meet the validation requirements of each service and JCIDS.

The second was, the process shall produce a requirements document that works to close a capability gap on the approved IPCL while the identified threat that generated the gap is still relevant.

The third MOE was, the process shall consider the impact to each of the services existing requirements needs, fielded systems, and technology efforts in order to not duplicate effort or cause negative impacts to each of the existing service efforts.

This third MOE while not necessarily required to generate the document or close the gap was seen to be significant. Multiple stakeholder needs dealt with the duplication of effort and the desire to not have efforts their service was already working negatively impacted. While the goal is to have the best solution for all four services, the political impacts must be considered as they have high impact on the success of the process. As seen from the requirements, there were several levels of approval in each of the four services that will be looking at these political impacts. As discussed by Hitchins, in his rigorous soft method (RSM), complex problems often have several root causes which are not always part of the system, but which may impact it (Hitchins 2019). This third MOE falls under the term POETIC which Hitchins defined as Politics, Organization, Economics, Technology, Inertia/Inactivity, and Culture. These items play a part in the JEOD requirements process which was shown by the stakeholder needs and resulting requirements.

The JEOD requirements process is not a system which is fielded in an operational environment, but it does have to be suitable for the organizational structure of JEOD. Therefore, the first MOS was the process shall be adaptable for both urgent and deliberate threat requirements.

The second MOS was the process shall be able to be performed by a single requirements writer with input from the MTAB.

10. Analyzing Requirements

As the requirements had already gone through one round of analysis to group them and develop MOEs and MOSs, the next analysis step was to ensure that each stakeholder need was covered by a requirement. The analysis was performed in Innoslate. Each requirement was traced back to the stakeholder need that was it related to. A traceability matrix was produced and shown in Appendix A, Figure 60. Each of the stakeholder needs was captured by a requirement. The stakeholder needs that had the most requirements traceability were those that dealt with ensuring all the required documentation was provided to allow for JCIDS and single service validation. Having an efficient and effect process were close seconds.

When the requirements were analyzed, a similar pattern emerged. Impact to existing systems and interoperability with existing systems had the most overall, while timeline and gap closure were close seconds. This seemed to imply that it was more important to the stakeholder to ensure there was no negative impact to existing single service efforts than it was to have an efficient process or to effectively close the gap. This lined up with what was seen when researching previous JEOD requirements efforts. It is essential to prioritize the upfront research to ensure there is no technology overlap otherwise the process may not succeed even if it closes the gap in a timely manner.

There were a few requirements that did not have a corresponding stakeholder need. These were to have an iterative process that incorporated systems engineering and agile processes as well as EOD technician input that could handle urgent and deliberate needs. These were added requirements based on the analysis of the current process. Their addition should be considered when developing the new process.

11. Recording in Database.

It was noted from the traceability matrix that a need for a database was not specifically called out as a stakeholder need or requirement. There was a requirement to have a repeatable process. The repeatable process requirement stated that the process shall designate what parts are repeatable. MBSE could be one way to meet this requirement.

B. DEVELOPMENT OF NEW JEOD REQUIREMENTS PROCESS

1. Process Boundary

The first step of developing the new process was to define the boundaries of the new process. From Figure 20, there were four main steps in the current JEOD process. They were the threat analysis, capability gap definition, requirements documents, and JCIDS. From the analysis of the current JEOD process, the first step of threat analysis generated a prioritized threat list which kicked off the capability gap definition. There were no changes required to this part of the process. Likewise, the final step of JCIDS was a set process that could not be changed. These two steps were left in the new process but not modified. The four main steps in the JEOD process were not changed at a high level but modified at lower levels as shown in Figure 22.

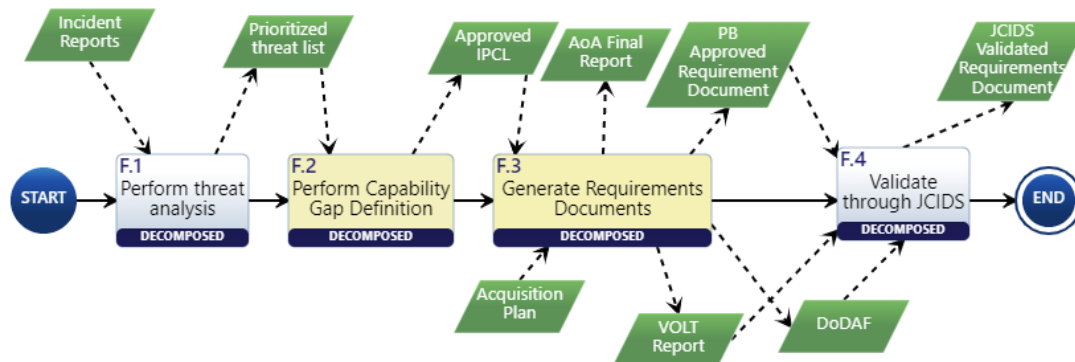


Figure 22. New JEOD Requirements Process Top Level

2. Changes to Existing Process Steps

As shown in Figure 22, the new JEOD requirements process was modeled in Innoslate. Unchanged steps from the current process were shown as white blocks and unchanged inputs and outputs were shown as green blocks. Steps that were changed or added were shown in yellow and new inputs and outputs were shown in blue.

a. *Changes to the Capability Gap Definition Process*

The current capability gap definition took the prioritized threat list and used it to populate CBVM, identify gaps, and generate scenarios as shown in Figure 23.

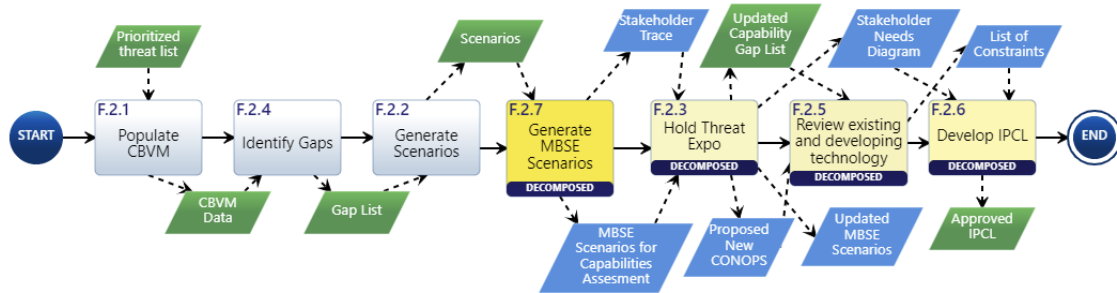


Figure 23. New Capability Gap Definition Process

As they already were well defined, the first three steps were left unchanged. After the scenarios were generated, a new step was added to model the scenarios with MBSE. As seen from Figure 24, part of modeling the scenarios was to identify and analyze the stakeholders and enabling systems for each scenario.

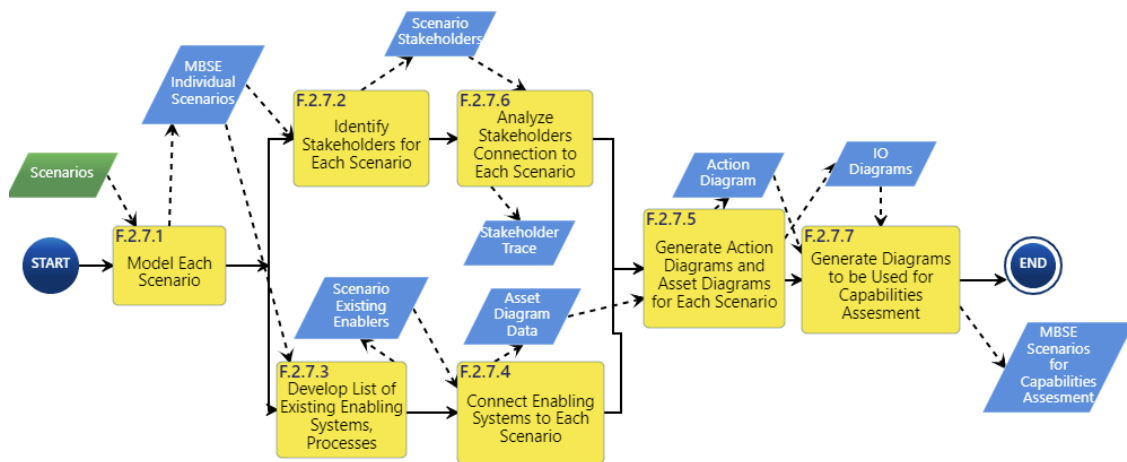


Figure 24. New Step to Generate MBSE Scenarios

This data was used to produce action, asset, and IO diagrams that could be used as part of the threat expo and later requirements generation steps. It provided a visual representation of the scenarios and accomplished steps 1 and 2 from Table 1 which was the systems engineering process chosen as a guide for development of the new process to align it with systems engineering best practices.

The threat expo portion of the process was also updated as shown in Figure 25.

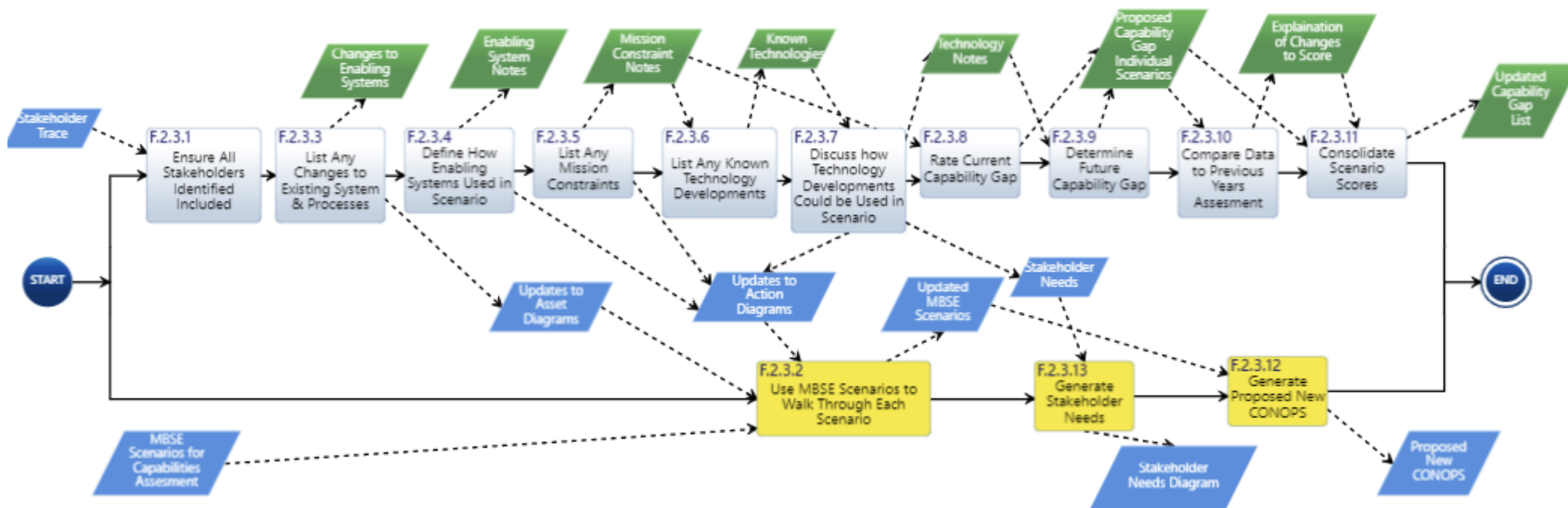


Figure 25. Modified Threat Expo Process

In order to keep the existing process which works well unaffected, an additional step was added parallel to the existing threat expo to capture the data in the already created MBSE models. A new step of using the data to develop the stakeholder needs and CONOPS was also added concurrent to the existing process. These steps would be performed by the JEOD Requirements Writer. Adding these steps covered steps 3–5 on Table 1. This was also the point in the process in which CONOPS were generated which was identified in the Monterey Phoenix analysis as a critical component for developing the CDD.

The CONOPS were used to feed the process for reviewing existing and developing technology. As shown in Figure 26, the CONOPS were used to model how the potential technology solutions found from the industry day could be used to help develop the Battle Lab events and met step 6 from Table 1.

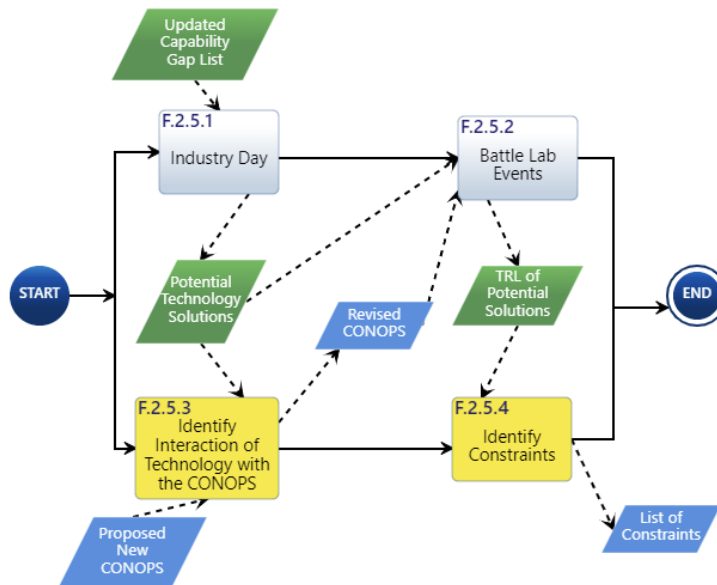


Figure 26. Modified Technology Demonstrations

The results from the Battle Lab events were then fed back into the models to identify where the technology readiness level (TRL) did not meet the needs of the CONOPS which could be identified as constraints, step 7 from Table 1.

At this point, the IPCL was developed in the same manner as the current process. Now however, there were two new inputs of the list of constraints and the stakeholder needs diagram which could feed the existing process as shown in Figure 27.

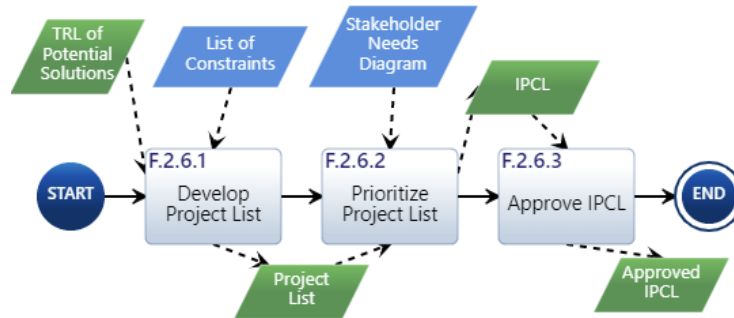


Figure 27. Modified IPCL Process

These steps added traceability back to the original stakeholder needs as well as recorded technology constraints.

It was important to note that up until this point, the process was capturing data for all the capability gaps. After this point, the process shifted to looking at developing requirements for one capability gap at a time. However, all the upfront data would be retained for each capability gap for future use.

b. Changes to the Generate Requirements Documents Process

As shown in Figure 28, the overall Requirements Generation process was left unchanged, but modifications were made to several of the steps.

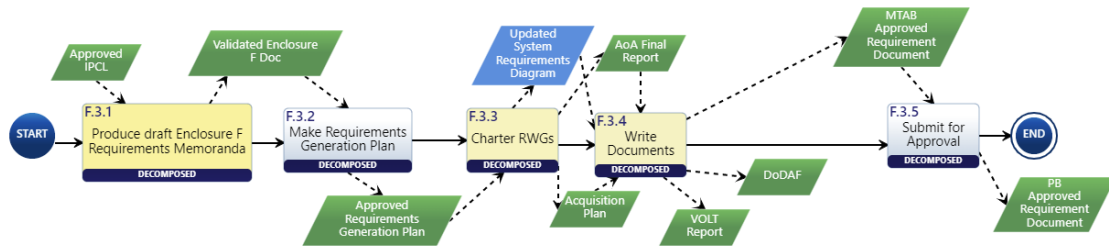


Figure 28. New Requirements Generation Process Step

(1) Changes to the Produce draft Enclosure F

The first process modified was the production of the Enclosure F Requirements Memorandum (Encl F). The Encl F was a significant step in the process as it was where the stakeholder needs and requirements were defined. Since JEOD used the Encl F in place of capability specific ICDs, the Encl F had to fill the role of the capability specific ICD. As seen from Figure 29, the process already had steps to write the Encl F. What it did not have was steps to show where this data should come from. These were the steps that were added.

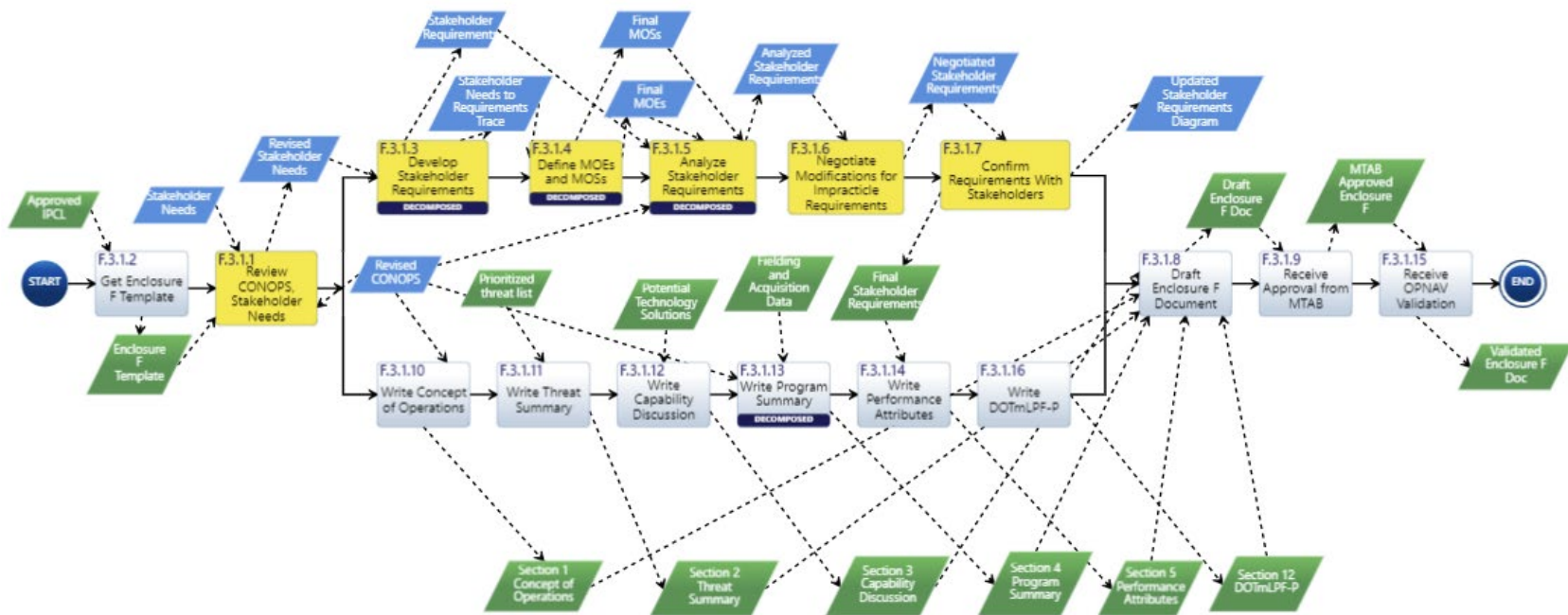


Figure 29. Modified Enclosure F Process

First, a step was added to review the CONOPS and stakeholder needs. As discussed in Chapter II, the requirements process is iterative with the stakeholder needs continuously referenced to ensure the requirements continue to be defined correctly. In addition, this allowed the process to be adaptive to changes that may occur during the course of the process and get stakeholder concurrence that the requirements still meet the CONOPS as discussed in Figure 5.

Instead of just writing the document sections shown in the bottom portion of Figure 29, the systems engineering process was followed on the top line to generate the data that would go into the sections on the bottom line.

The first step on the top line in Figure 30, was to develop stakeholder requirements. As discussed by Walden et al. 2015 and INCOSE 2012, this step translated the stakeholder needs from the users perspective to stakeholder requirements from the suppliers perspective, step 8 in Table 1.

As discussed by Ulrich and Eppinger 2016, determining latent needs was critical to ensure that the stakeholder would accept the system. In order to do this and also to capture the stakeholder's motivation, the adaptive process format of a CARD was incorporated into the process (Sharma 2017) as shown in Figure 30. Figure 30 is a breakdown of the develop stakeholder requirements block in Figure 29.

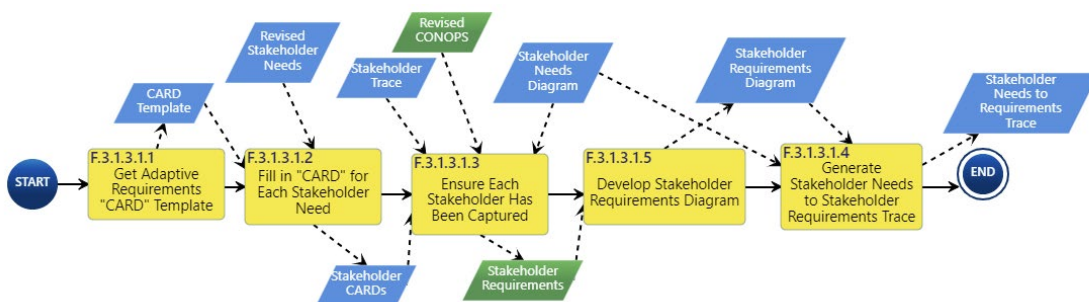


Figure 30. Develop Stakeholder Requirements Steps

The process again contained an iterative step to ensure the stakeholder requirements aligned with the CONOPS. All the data was captured in models to document the data.

On the top line of Figure 29, a new step was added to define Measures of Effectiveness (MOEs) and Measures of Suitability (MOSs) which were not done in the previous process. As discussed by Reese 2018 and the DAG, it was important to capture the mission objectives in a way that could be used to evaluate if the system met them. Figure 31 showed the steps to develop the MOEs and MOSs. From the analysis done in developing the JEOD process, it was seen that using a stakeholder needs to requirements trace was a useful tool to identify the most important requirements and the hardest to achieve stakeholder needs. Therefore, this trace was added as a tool to use in generating the MOEs and MOSs.

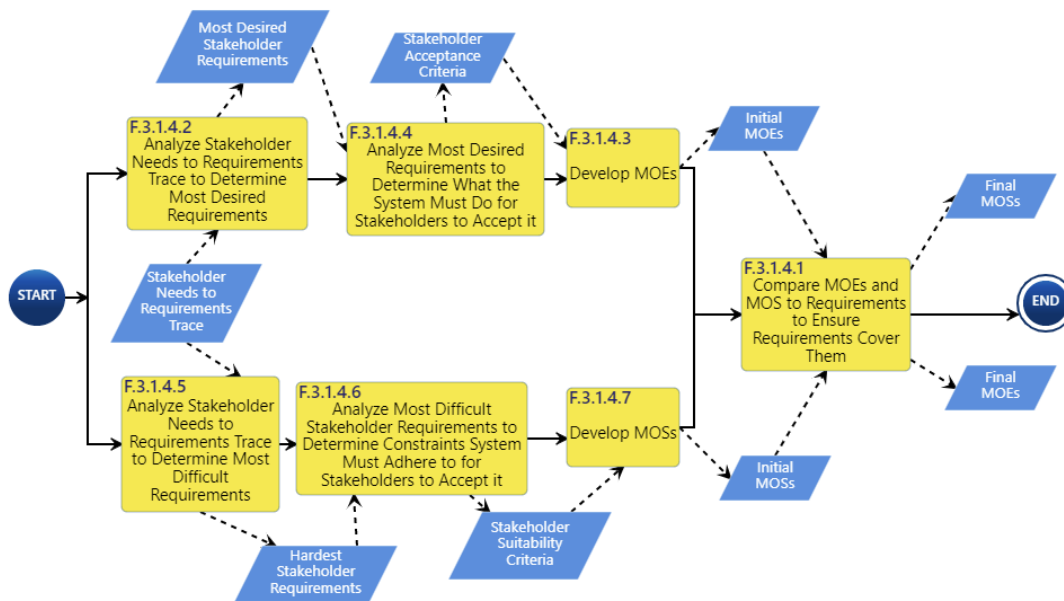


Figure 31. Define MOEs and MOSs Steps

The next step was to analyze the stakeholder requirements. As shown in Figure 32, the stakeholder requirements were again compared to the CONOPS. They were also compared to Figure 7 from *ISO29148* to ensure all areas were considered and to *INCOSE 2012* to ensure they were written appropriately.

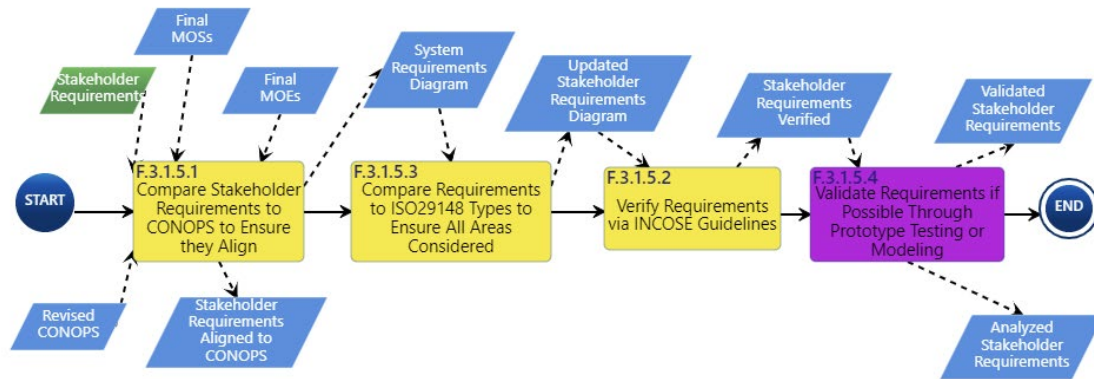


Figure 32. Analyze Stakeholder Requirements

Of note in Figure 32 was the last block which was highlighted in purple. According to INCOSE 2012 and Reese 2018, requirements should be validated to ensure that they as a whole satisfy the MOEs. However, this normally could not be done until a system was developed at the top right of the Vee diagram. Pushing the validation sooner in the process could catch infeasible requirements sooner. This step was inserted into the process to be used as possible to perform this check sooner in the process. Its use and methods were left undefined and were an area for future work.

Once the stakeholder requirements were analyzed, they were negotiated with the stakeholders to resolve any impractical requirements and then inserted into the Encl F and recorded in a database for tracking. This concluded the Encl F process as well as the stakeholder requirements generation process from Table 1.

(2) Changes to the Charter RWGs Process

The next step of the requirements generation process changed was the Charter RWGs process. As shown in Figure 33, several steps were added to the Charter RWG process. They covered steps 1–14 in Table 1 and followed the INCOSE System Requirements Definition Process (Walden et al. 2015).

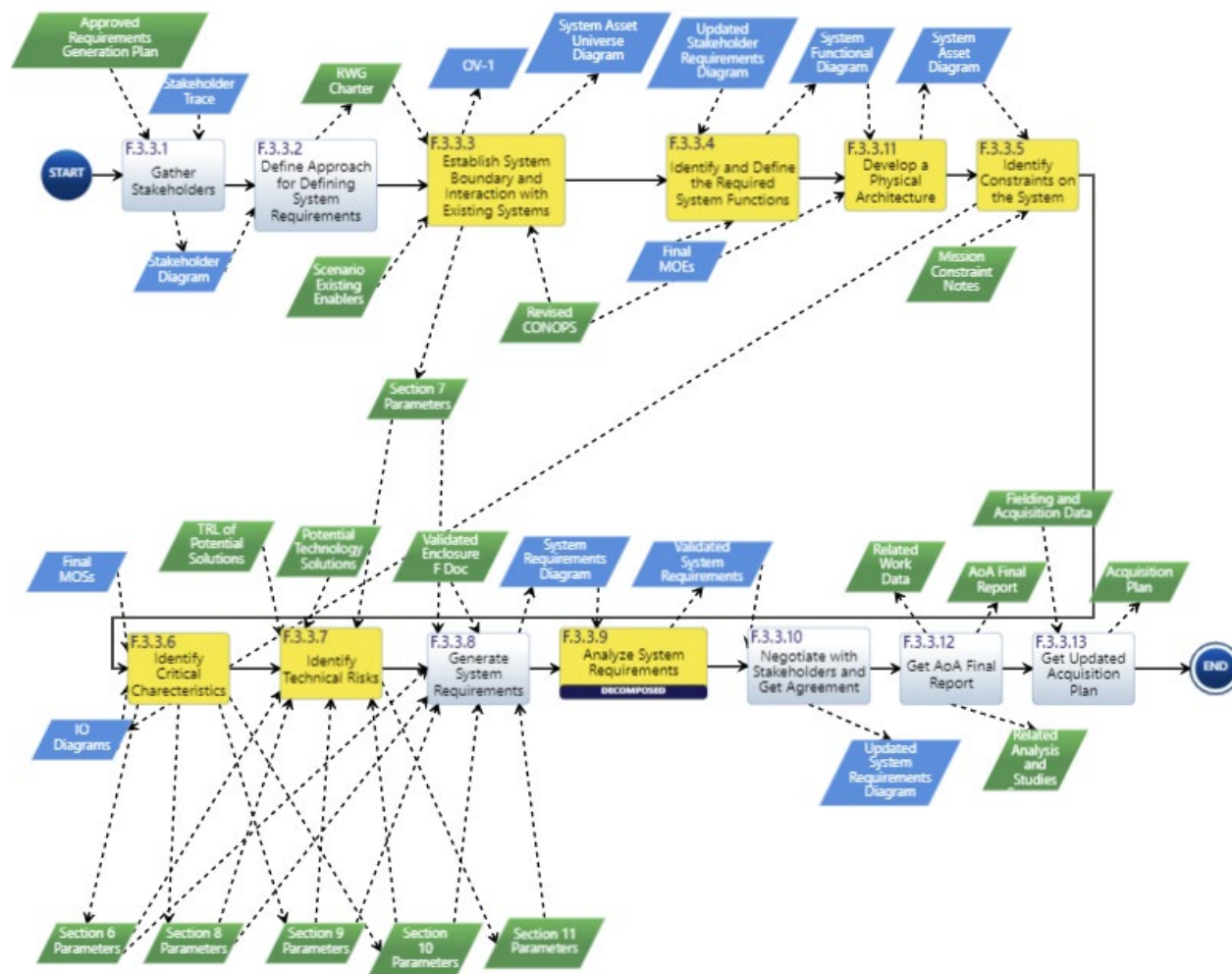


Figure 33. Modified Charter RWG Process

Figure 33 showed that the CONOPS again played a role in the process to ensure the requirements continued to align with them. The data from the generation of the Encl F and all the data from the model was also pulled into the process as appropriate. This process was the key part of the process that generated the data that fed the AoA final report, acquisition plan, and the CDD. The generation of the DoDAF views was also incorporated into the process to show where in the process the data would be generated to feed the views.

One of the requirements of the JCIDS process was development of the DODAF document (Intellipedia 2021). Various sources containing information on DoDAF generation were reviewed. The JCIDS manual discussed what views were required to support the various requirements documents but did not provide direction on how to generate them. The *DoDAF Architecture Framework Version 2.02* had information on all the DoDAF viewpoints and what should be in them (Chief Information Officer 2022). This document laid out the details of what should be in the DoDAF but they do not relate it to the JCIDS requirements documents. Therefore, a comparison was done between the JCIDS CDD and the DoDAF to determine how they aligned. The comparison was done in Excel and is shown in Appendix B, Table 19.

The DoDAF to JCIDS comparison showed that certain views were required for certain sections and described the data that should be included to be relevant. In order to better see how this information tied together, the DoDAF views were added as artifacts to the Innoslate model.

(3) Changes to the Write Documents Process

The data from the Charter RWG process was fed into the write documents process which was shown in Figure 34.

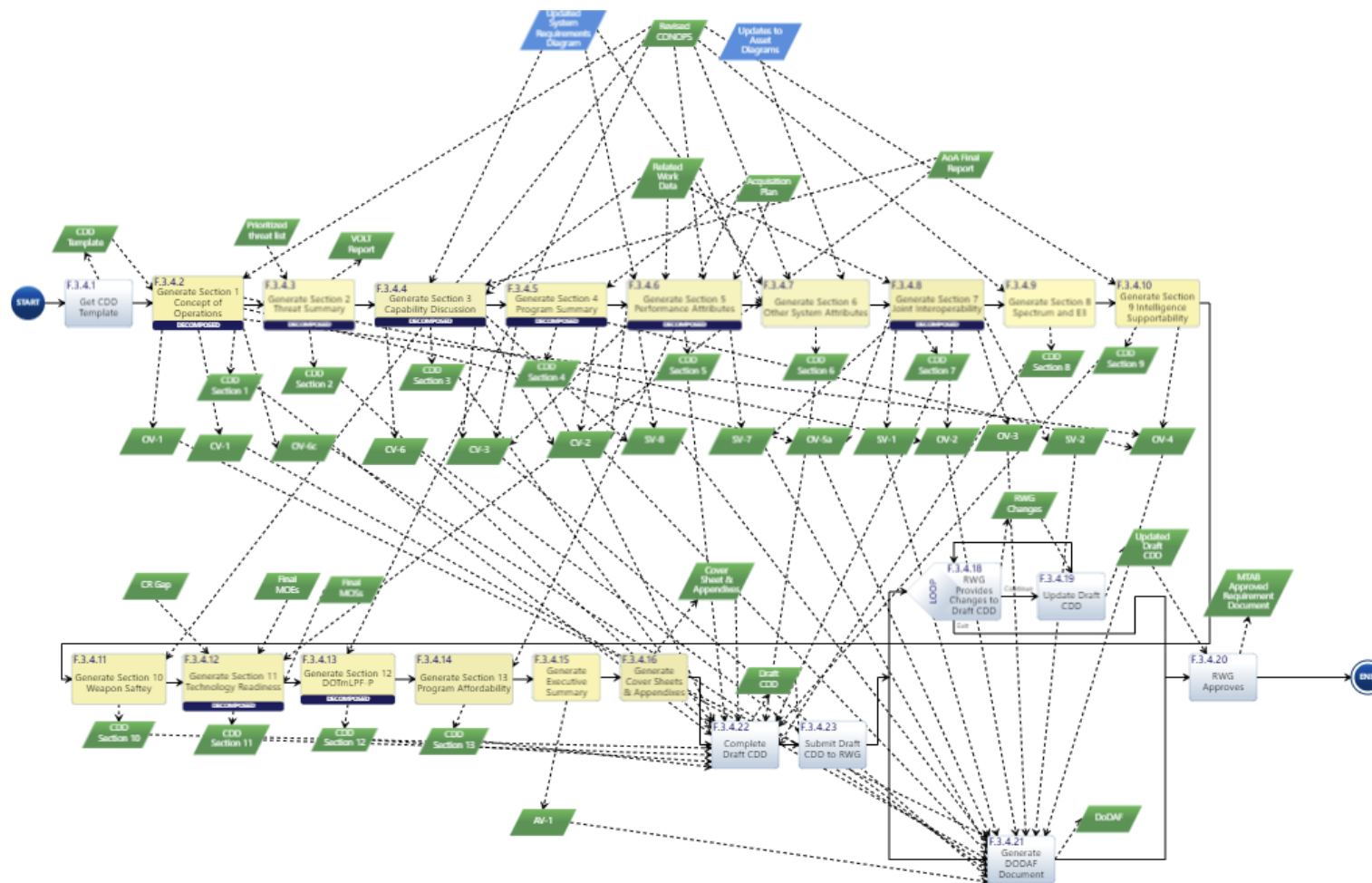


Figure 34. Modifications to Write Documents Process

Figure 34 was very complex with many interconnecting elements. This was in line with the analysis done in Monterey Phoenix which showed that CONOPS were critical component to writing many of the CDD sections. Similarities could be seen between Figure 34 and the JCIDS CDD Mapping shown in Appendix A Figure 58 that was used to come to this conclusion. Figure 34 showed how the prioritized threat list, related work, AoA Report, CR Gap, MOEs, and MOSs also supported the CDD. The models generated were also represented. Connections between each of the sections and the DoDAF views that would be generated were also shown to help the requirements writer know what data would support the generation of the views. Finally, Figure 34 showed which sections of the CDD would support generation of the VOLT Report.

3. Comparison of New Process Timeline to Old

Once the new process was developed, times were assigned to each of the new steps and Innoslate was used to run a Monte Carlo Simulation to determine how long the new process would take from start to end as shown in Figure 22. The mean time was found to be 1.53 years versus the 1.98 years for the current process. The comparison in times for each process were shown in Table 8.

Table 8. Comparison of New and Current JEOD Requirement Generation Timeline

Step	New Process Time	Current Process Time
Perform threat analysis	14 days	14 days
Perform capability gap definition	5.95 months	5.52 months
Generate requirements documents	7.7 months	1.13 years
Validate requirements documents	4.24 months	4.24 months

Table 8 showed that the capability gap definition timeline increased by half a month while the requirements documents timeline decreased by 6 months. These two areas were further compared in Table 9.

Table 9. Detailed Comparison of Current and New Requirement Document Timelines

Step	New Process Time	Current Process Time
Perform capability gap definition	5.95 months	5.52 months
Populate CBVM	14 days	14 days
Identify Gaps	28 days	28 days
Generate Scenarios	7 days	7 days
Generate MBSE Scenarios	7 days	NA
Hold Threat Expo	12.5 days	7 days
Review Existing and Developing Technology	1.86 months	1.84 months
Develop IPCL	1.84 months	1.84 months
Generate Requirements Documents	7.7 months	1.13 years
Produce Enclosure F Requirements Memorandum	1.17 months	28 days
Make requirements generation plan	4.84 months	4.84 months
Charter RWGs	8 days	28 days
Write documents	15.75 days	6 months
Submit for approval	28 days	28 days

Table 9 showed that the biggest decrease in time came from the step of write documents which went from 6 months to 15.75 days. In order to determine why this occurred, Figure 34 was analyzed in Innoslate. The analysis showed that the reduction in time occurred due to the fact that the data required to write the CDD was generated earlier in the process. The data for the concept of operations which drove most sections of the CDD now occurred in the Capability Gap Definition process step. The development of a MBSE database also occurred in this step concurrent with the already existing tasks.

The timeline for the Encl F generation was slightly increased to allow for 6 sections of the CDD to be drafted during this step versus in the write documents step. Therefore, the last step of writing the document only had to assemble the already existing data and ensure no changes had occurred.

The use of MBSE also allowed all the data from the threat and capability gap steps to be carried over for future use. All these items together allowed the new process to be about 5 months faster than the old process.

Additionally, the new process followed a documented systems engineering process which could be repeated on future requirements documents. Also, unlike the current process, the data from the capability gap definition process could now be used for more than one requirement document. Where it took nearly 2 years to generate one requirements document under the current process, the new process could generate two documents in nearly the same time frame as shown in Figure 35.

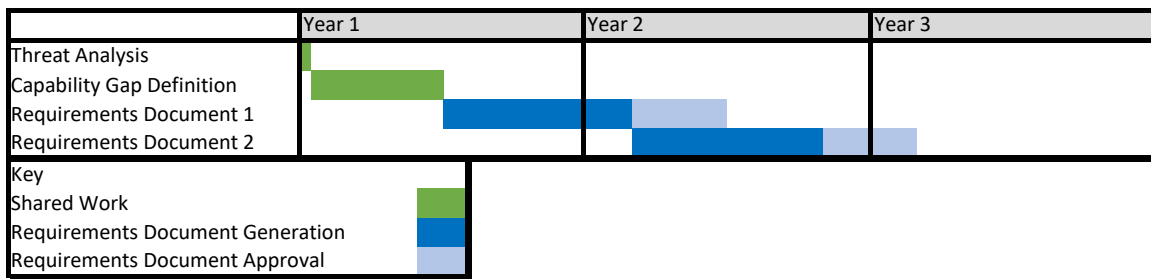


Figure 35. Comparison of Timelines

There is one caveat to these numbers in that the number of cycles allowed for the RWG to review the draft CDD was held to one. If multiple cycles were added the timeline would increase. This would have applied to the current process as well.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RAPID LARGE AREA CLEARANCE REQUIREMENTS ANALYSIS

The third part of this thesis and its second objective were to apply the new process to the use case of RLAC. Similar to Chapter III and as seen in Figure 36, this chapter contains 2 major sections: (1) the results of the stakeholder analysis to develop concept of operations and stakeholder requirements, and (2) the results of the requirements analysis and resulting proposed architectures.

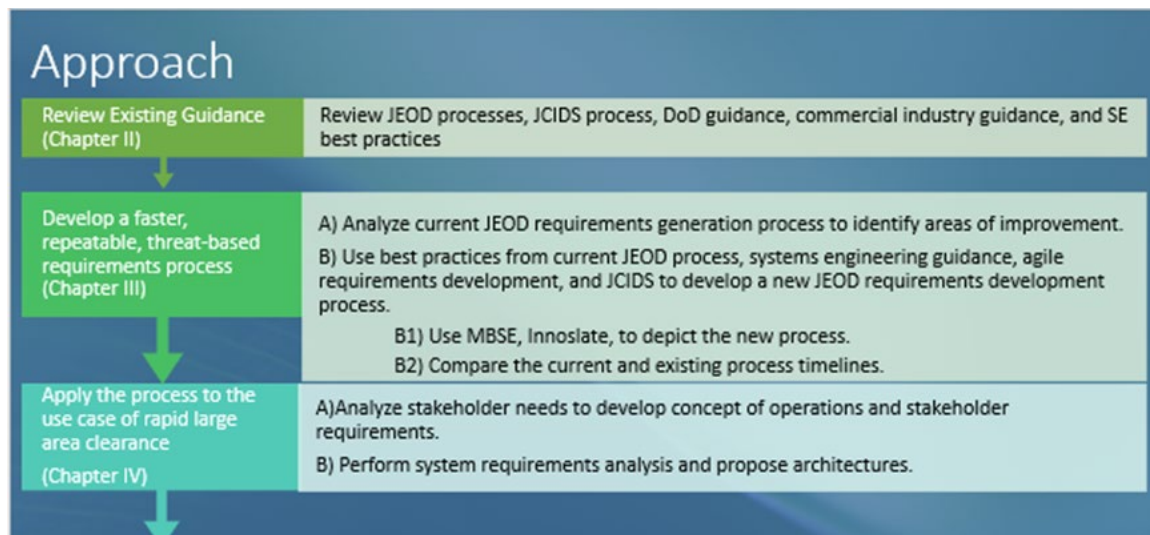


Figure 36. Chapter IV Steps Taken

Section A describes the generated stakeholder needs for RLAC and explains how they were used to develop CONOPS and stakeholder requirements. Like Chapter IV, the SE process from Table 1, Stakeholder Needs and Stakeholder Requirements Process was used as a guide. Section B explains how the analysis followed the steps in Table 1, System Requirements Process and ended with proposed architectures versus going all the way to system requirements.

An abbreviated process was used given the time constraints of this thesis. The material gathered was also kept unclassified from open sources. Therefore, the parts of the process specific to JEOD such as the threats analysis were not applied. While the scope

was limited to developing stakeholder requirements and proposing an architecture, existing JEOD and other service requirements were compared to the RLAC stakeholder requirements to determine if there was enough commonality to have a repeatable threat-based process and to determine how to write a requirements document that had the best chance of resulting in a fielded system.

A. STAKEHOLDER NEEDS ANALYSIS

1. Identifying Stakeholders

The first step taken was to define the stakeholders for RLAC. This step fell under the Perform Capability Gap Definition Process, Hold Threat Expo, as shown in Figure 24. The stakeholders were the same as those for the JEOD process shown in Figure 14. While the stakeholders did not change, their roles did change in some cases. Primary stakeholders were defined as those that had a direct role in developing the requirements while secondary stakeholders were only involved in the process.

Table 10. JEOD Stakeholders

Stakeholder	Role in Process	Role in Development
Sponsor – OPNAV	Primary	Primary
Gatekeeper - USN	Primary	Secondary
Stakeholders - JCIDS	Primary	Secondary
Functional Capabilities Board	Primary	Secondary
Joint Capabilities Board	Primary	Secondary
Requirements Offices – From each of the 4 services	Primary	Primary
Program Board / Action Officers	Primary	Secondary
MTAB	Primary	Primary
ERB	Secondary	Primary
TTAB	Secondary	Secondary
NAVSCOLEOD	Secondary	Secondary
EOD Technicians – From each of the 4 services	Secondary	Secondary
Program Offices – From each of the 4 services	Primary	Primary
Technology Developers – From each of the 4 services	Secondary	Primary
Industry	Secondary	Primary
JEOD T and T	Primary	Primary
ONR	Primary	Primary
Other DOD Technology Developers	Secondary	Primary

Stakeholder	Role in Process	Role in Development
Academia	Secondary	Secondary

OPNAV and MTAB continued to be primaries as well as requirements and program offices from the other four services, JEOD T and T, and ONR. Added primaries were ERB and technology developers. These were the people that should be involved in writing the documents. It was interesting to note that the primary stakeholders in the JEOD requirements process that were involved in the approval of the document were not always the same as the primaries generating the data to write the document. Care should be taken when writing the document to not forget about the primary stakeholders from the overall process. Even if the primary stakeholders involved with writing the document are happy with it, the document will not be approved without the buy in from the primary stakeholders in the overall process. Their needs must not be forgotten while gathering the data to generate the documents. The JEOD requirements process laid out in Chapter III was laid out to capture the overall stakeholder needs as part of the new process.

2. Identifying Enabling Systems and Processes

The next step also from Figure 24, was to identify enabling technologies. There were several existing technologies already fielded and in development that could be used for large area clearance. They were shown in Figure 37.

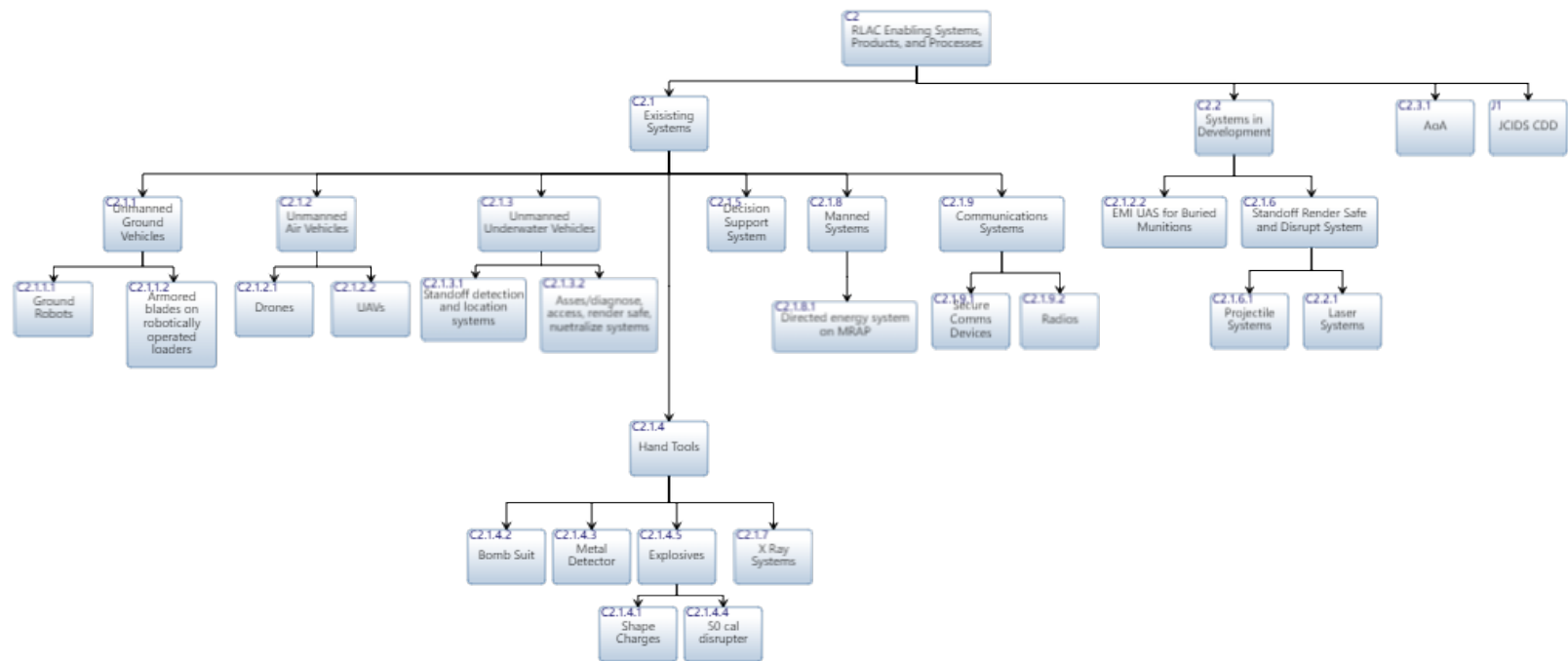


Figure 37. RLAC Enabling Technologies

Systems used by the DOD were referenced in general terms and were further described below.

The Army had developed an unmanned ground robotic vehicle. Its purpose was to provide standoff distance for services to detect and confirm presence, identify disposition, and counter hazards, specifically for chemical, biological, radiological and nuclear (CBRN) (USAASC 2022). The unmanned system developed by the Army was intended to detect and neutralize explosive hazards to clear remote dangerous areas. It is currently used by the USA, USN, and USMC for EOD missions.

The USAF used the Remote Mass Mechanical Clearance (RMMC) armored clearance blades mounted on robotically operated and hardened wheel loaders and compact track loaders (Goddin 2017). These systems were designed to clear surface UXOs and explosive residue components from paved surfaces via remote operation. They were not designed to be expeditionary.

The USN also had several ground robots deployed, as shown in Figure 38.



Joint Service EOD Robots



Robotics (Medium):

- Man-Transportable Robotic System (MTRS) II
- Tactical operations; transported to incident in EOD response vehicle; intended for in-depth recon and hazardous item prosecution



Robotics (Small):

- Dismounted operations; lightweight & backpackable; initial recon usage



Robotics (Large):

- Common Robotic System-Heavy (CRS-H)
- Base/Infrastructure operations; transported in large response vehicle; intended for max lift, widest-range of neutralization/render safe operations



Flexible Cyber Secure Radio (FlexCSR)

- Flexible, cybersecure radio with the ability to operate securely in four re-configurable spectrum bands

Distribution A: Approved for Public Release. Distribution Unlimited.

Figure 38. The Robots Deployed. Source: Malatesta (2021).

For UAVs, the USAF also had a program, Rapid Airfield Damage Assessment System (RADAS) which used Small Unmanned Aircraft (SUAS) to sense damage rapidly and remotely on a runway (JBER Public Affairs 2019). According to the USAF, the RADAS was, “designed to significantly reduce hazardous exposure operators might encounter, as well as reduce the time the airfield recovery and assessment process takes” (JBER Public Affairs 2019). The USAF also stated that the RADAS was designed to assess runway damage and locate UXO.

The USN also had requirements related to RLAC but for underwater versus surface applications. The first was the Maritime Expeditionary Countermeasures (MCM) Unmanned Undersea Vehicle (MEMUUV) (Lundquist 2021). The MEMUUV addressed the steps of detect, locate, classify/identify, and acquire/re-acquire in the subtasks for successful completion of threat response missions. These aligned with the RLAC steps of

detect, locate, and identify. The MEMUUV was classified by Lundquist as a medium system which would not align with expeditionary missions. He discussed that smaller systems were in development.

While the MEMUUMV performed the sub-tasks of detect, locate, classify/identify, and acquire/re-acquire, the Maritime Expeditionary Standoff Response (MESR) FoS performed the sub tasks of asses/diagnose, access, render safe procedures, and neutralize (Malatesta 2021). This was similar to the RLAC tasks of access and render safe/neutralize. MESR was designed to be an incremental FoS with payloads that were field configurable and interchangeable. An overview of the Navy's plans for UUV deployment was shown in Figure 39.

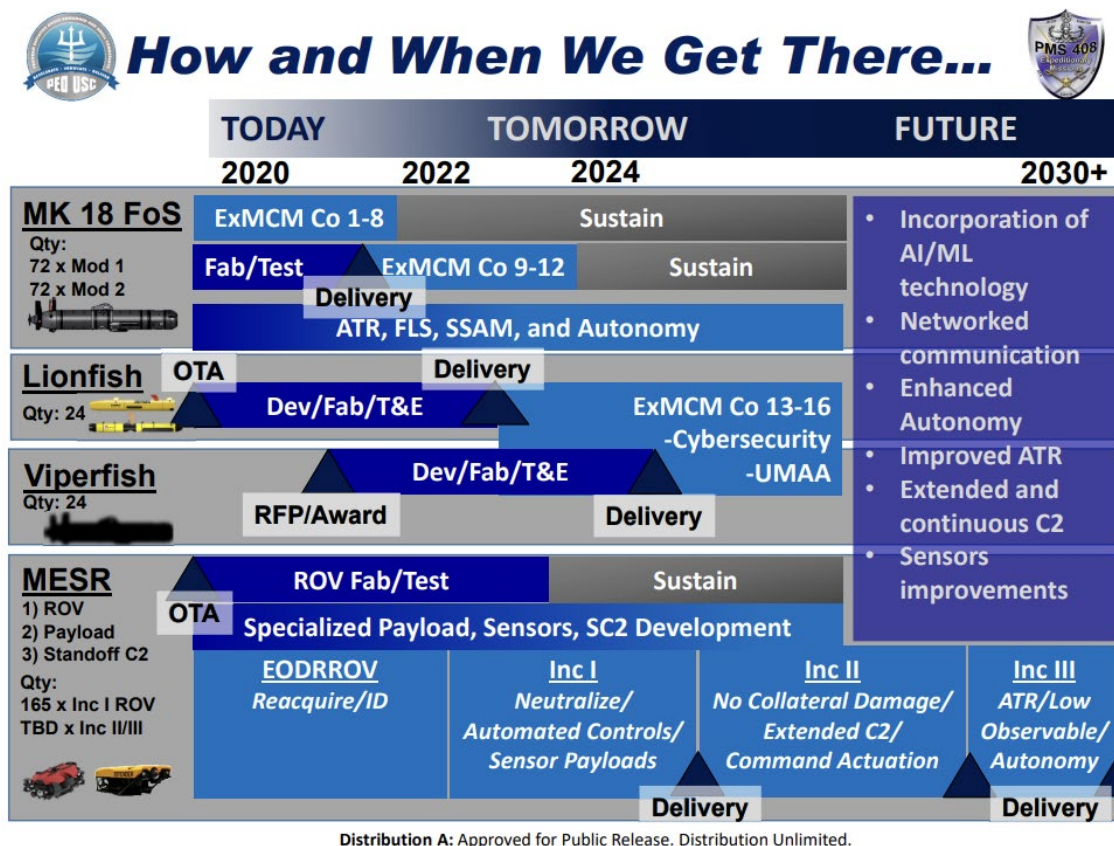


Figure 39. USN UUV Plans. Source: Malatesta (2021).

The USN under JEOD also has several existing systems that were used directly by the technicians. A bomb suit could be worn during operations but was cumbersome and only worn for short periods. Metal detectors could be used by hand to find buried items or mounted to unmanned systems. Explosive devices could be used to disrupt or render safe items. X ray systems could be used to identify the internals of IEDs and UXO to determine correct position of render safe tools. JEOD also used the Decision Support System (DSS) which was designed to support EOD operations by providing near real-time information via mobile applications (Malatesta 2021). Finally, the USN was developing a standoff render safe and disrupt system (SRSD), access buried munitions systems, and an RLAC system (Malatesta 2021).

There were also systems that could be mounted on manned vehicles such as the Recovery of Airbase Denied Ordnance (RADBO) system being developed by the USAF (Brackens 2022). According to Brackens, the RADBO was a 3 KW fiber optic laser directed energy system with a remote-controlled interrogation arm mounted on a Mine-Resistant Ambush Protected (MRAP) light tactical vehicle. Its purpose was to use directed energy to safely detonate IEDs or UXOs in deployed or austere locations (Brackens 2022).

In order to allow unmanned vehicles to safely transmit secret data, the USN developed the Flexible Cyber-Secure Radio (FlexCSR) which used a security cyber module (SCM) and cryptographic unit (ECU) (Nguyen et al. 2019).

3. Gathering Stakeholder Needs

The stakeholders and enabling systems were mapped in Innolsate and used to generate asset and action diagrams. These were then used to discuss how the technology could be used for RLAC and to generate stakeholder needs. The stakeholder needs were shown in Appendix B, Table 20. While the stakeholder needs were listed by stakeholder, they were not provided by the actual stakeholders. Rather, they were generated using personal knowledge of the program.

While not shown in Appendix B Table 20, all the stakeholders required funding to perform their work. This could be a major driver in the effort. Without funding, all work stops.

Next, the stakeholder needs were analyzed. The first things that was apparent was that the needs were split into two groups. The first were needs that were specific to the RLAC system. These were the things the RLAC system was required to do. The other group of stakeholder needs were more about the information/items needed to approve the RLAC requirements, develop, procure, and support the system. These were grouped under process needs.

The stakeholder process needs were rearranged using Innoslate to group like needs. When this was done, an interesting pattern emerged. As the needs were grouped, they began to align with the various sections of the CDD. These were shown in Figure 40.

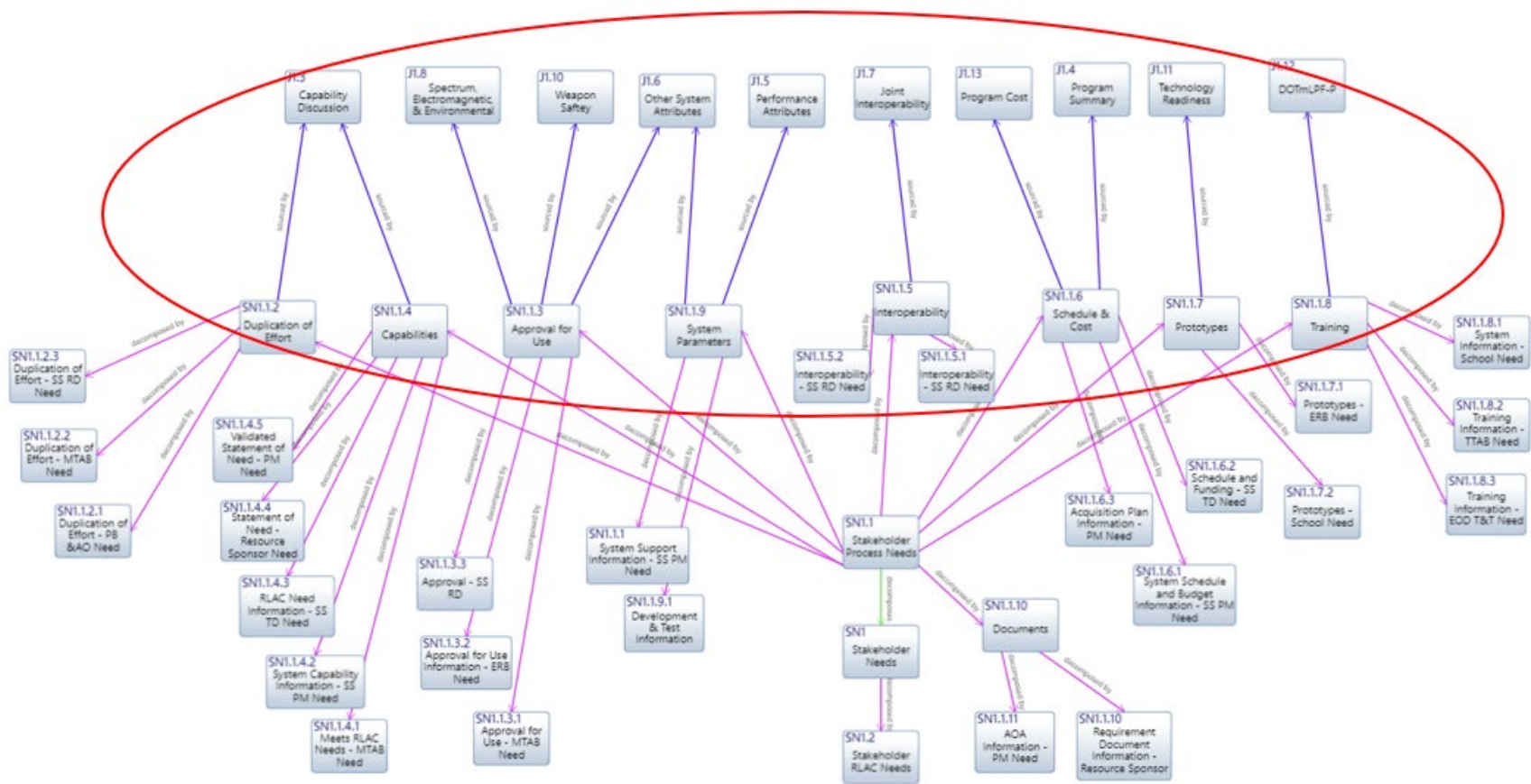


Figure 40. Stakeholder Process Needs and JCIDS CDD Alignment

Section 1, Concept of Operations lined up with the RLAC needs that described what the system had to do. The same applied to Section 2, Threat Summary. Section 3, Capability Discussion aligned with the needs that spoke to duplication of effort and capability gap. Section 4, Program Summary lined up with schedule and cost needs which also applied to Section 13. Section 5, Performance Attributes lined up with system parameters which would come from RLAC needs and also lined up with information needed for development, test, and support. Section 6, Other System Attributes lined up with system parameters which would come from RLAC needs. It also lined up with information needed for development and test as well as with some of the approval for use needs. Section 7, Joint Interoperability lined up with interoperability needs. Section 8, Spectrum, Electromagnetic, and Environmental lined up with the approval for use needs as well as the RLAC needs. Section 9, Intelligence was an exception as it was not represented by any of the stakeholder needs. Section 10, Weapon Safety lined up with the approval for use needs. Section 11, Technology Readiness lined up with the prototypes needs and Section 12, DOTmLPF lined up with the training needs.

This demonstrated that each of the user needs had a section in the CDD where it would need to be addressed. This was also useful in that it showed the requirements writer which stakeholders have a vested interest in each section of the CDD. This could be used to help gather the correct information for each section to make sure that the stakeholders needs are being captured and addressed. As the process needs were independent of the specific system needs, this also showed that if a process can be mapped out that showed where to gather the appropriate information for each section in the CDD, that portion of the process could be repeatable which was an objective of this thesis. The same applied to the RLAC needs. Even though other capabilities would have different information, Sections 1, 2, 5, 6, and 8 in the JCIDS CDD would still be the sections most closely linked to the functions of the system. This information was incorporated into the new JEOD process during the development of the stakeholder requirements.

The other interesting item noted was that the AoA information and the requirement document information were linked. The AoA needed information from the requirements documents and the requirements documents required information from the AoA. This

implied that the process to generate both of these documents would need to be iterative versus serial. This was also noted in the new process to show where each of the items would need to provide information to the other.

When the RLAC system needs were looked at specifically, it was seen that they fell under two main areas as shown in Figure 41. Functions the RLAC had to perform and constraints that affected how it performed those functions.

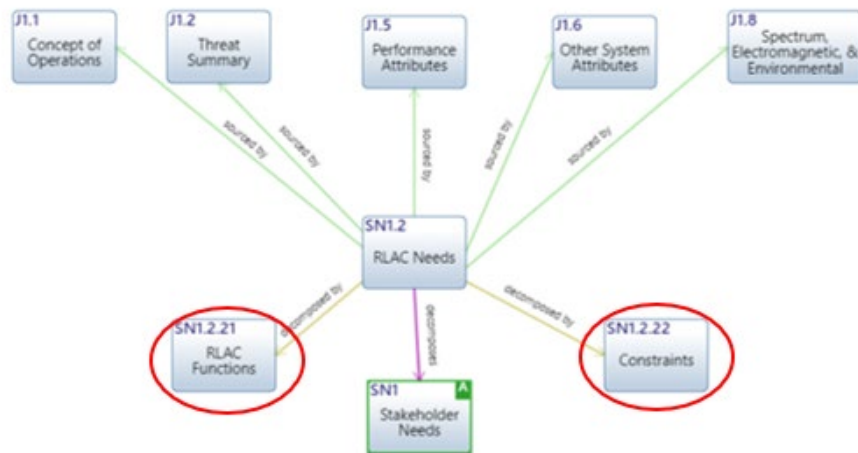


Figure 41. Stakeholder RLAC Needs and JCIDS CDD Alignment

The functions RLAC had to perform were plan mission, deploy to site, assess the situation, set safe area during mission, search for possible threats, provide location information, if found identify the threat, access threats if buried, take action against the threats as required, remove threats from the area if required, return to base, and report on actions taken. It was noted that many of these were if statements, Figure 42. They may not need to be done depending on the situation.

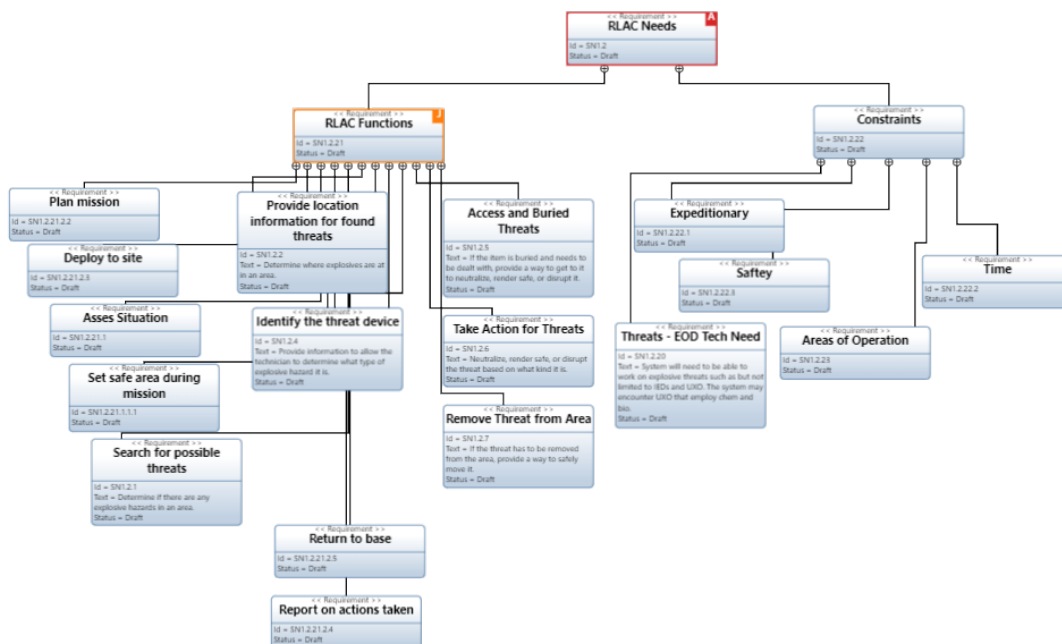


Figure 42. RLAC Functions

The constraints fell into the major areas of threats, expeditionary, time, safety, and areas of operation. They were further broken done as shown Figure 43.

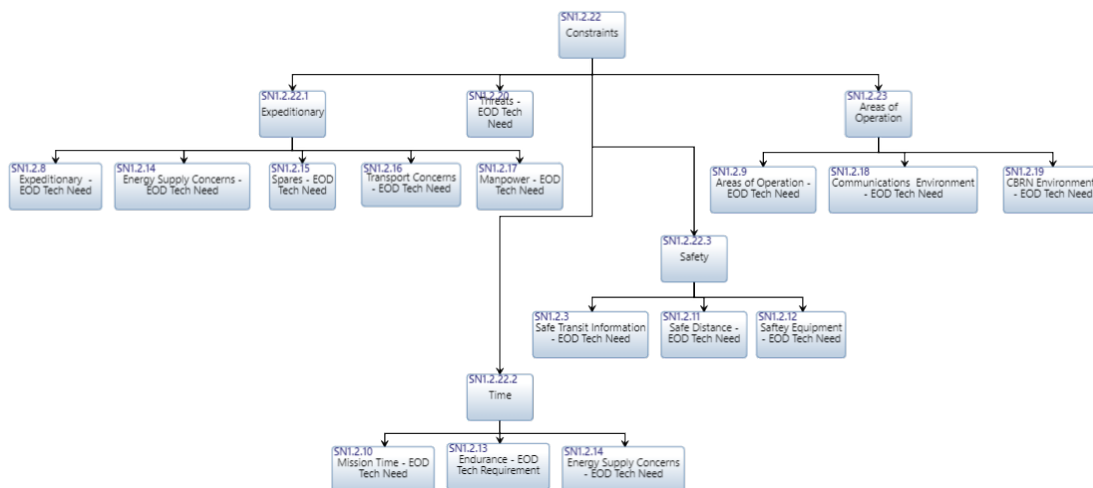


Figure 43. RLAC Constraints

The split between functions the system would have to provide and constraints on how it would provide them was significant as these would be used later to develop the functional model of the system.

4. Prioritizing Stakeholder Needs

Based on the previous analysis of the stakeholder needs, it was seen that the needs fell into two groups, needs that were needed as part of the process and those that were needed for the RLAC system itself. Analyzing the stakeholder needs for the process, it was seen that they were similar to those found in Chapter III for the JEOD requirements process. Like the stakeholder needs from Chapter III, avoiding duplication of effort and providing a needed capability when it was needed that could be procured and supported by each of the four services were the most important needs. This was followed by a system that could get approval for use from all of the four services and be interoperable with all of their existing equipment.

When looking at the stakeholder needs for the RLAC system itself in Figure 42, the constraints on the system were ranked a high priority as they would have to be met in order for the system to be used. The system would need to be safe to use against threats in typical EOD expeditionary areas of operation and timelines. As the functions it had to perform had several if statements based on the situation, the tasks that were always performed were ranked highest. These were plan the mission, deploy to the site, assess the situation, set the safe area, search for possible threats, return to base, and report on actions taken. If these tasks could consistently be performed within the EOD constraints, they would fill several of the RLAC needs namely allowing EOD technicians to determine if threats exist over a large area from a safe location.

The next highest priority tasks were those taken if a threat was found. These were provide location information and identify the threat device. Again, these would allow the EOD technician to safely determine what type of threat existed and where.

Finally, the if actions of access buried threats, take actions for threats, and remove threat from the area were ranked lower as they may not always need to be performed.

Based on the stakeholder needs and their priority, the next step was to come up with an overall stakeholder need which would capture the overall intent. The stakeholders had previously expressed their overall need as, “The ability to rapidly clear a large area of explosives.” Looking at all the stakeholder needs, the need for rapid, large area, and clearing of explosives were represented in the original statement. However, there were other important stakeholder needs that were not represented in the original statement such as considering the constraints of performing in the expeditionary environments EOD operates, performing the mission while minimizing risk to the operator, and producing the supporting documentation to ensure the system could be approved for use, fielded, and supported. Taking these other items into consideration, the overall needs statement was revised to, “The ability to develop, field, and support a system that can be used in expeditionary EOD environments to rapidly clear a large area of hazards while minimizing risks to the operator.”

5. Developing Operational Scenarios

Based on the stakeholder needs and knowledge of how the system may be used, operational scenarios were developed as part of the process, as shown in Figure 25. They were not based on input from the actual EOD missions in order to remain general to the overall rapid large area clearance problem that multiple organizations, even nonmilitary, might face. This was done to keep a broader perspective and keep the information unclassified.

As seen from the analysis in Chapter III, CONOPS were an essential part of the requirements writing process needed to generate a CDD. Other research had shown that CONOPS add value by, “helping scope the problem and solution, bridging where we are and where we want to be, illustrating how the system will function, facilitating communications among stakeholders, providing a logic trail of capability, providing a baseline for measuring system efficacy, and providing a baseline for requirements” (Edson, Robert and Frittmann 2010, 241). Edson discussed the ways in which CONOPS were underutilized as part of the requirements process which held true for the JEOD requirements generation process as well. In his paper Edson discussed the various ways

that CONOPS are viewed. He described that they are often only seen as a document for describing aspects of a military operation. However, they can also be used to describe how a system can be used as part of that mission.

The concept of operations developed as part of this thesis fell under the latter. It was not intended to describe the military operation to perform rapid large area clearance, but rather how the RLAC system could be used as part of that mission. While there was good documentation from the *IEEE 29148* on how to develop CONOPS documents and what should be in them, the CONOPS developed for this thesis were kept simple to align with the scope of this effort (IEEE 29148 2011). As part of an SE 4150 team project, several sets of CONOPS were developed by the team and then consolidated into an overall document which was shown in Figure 44.

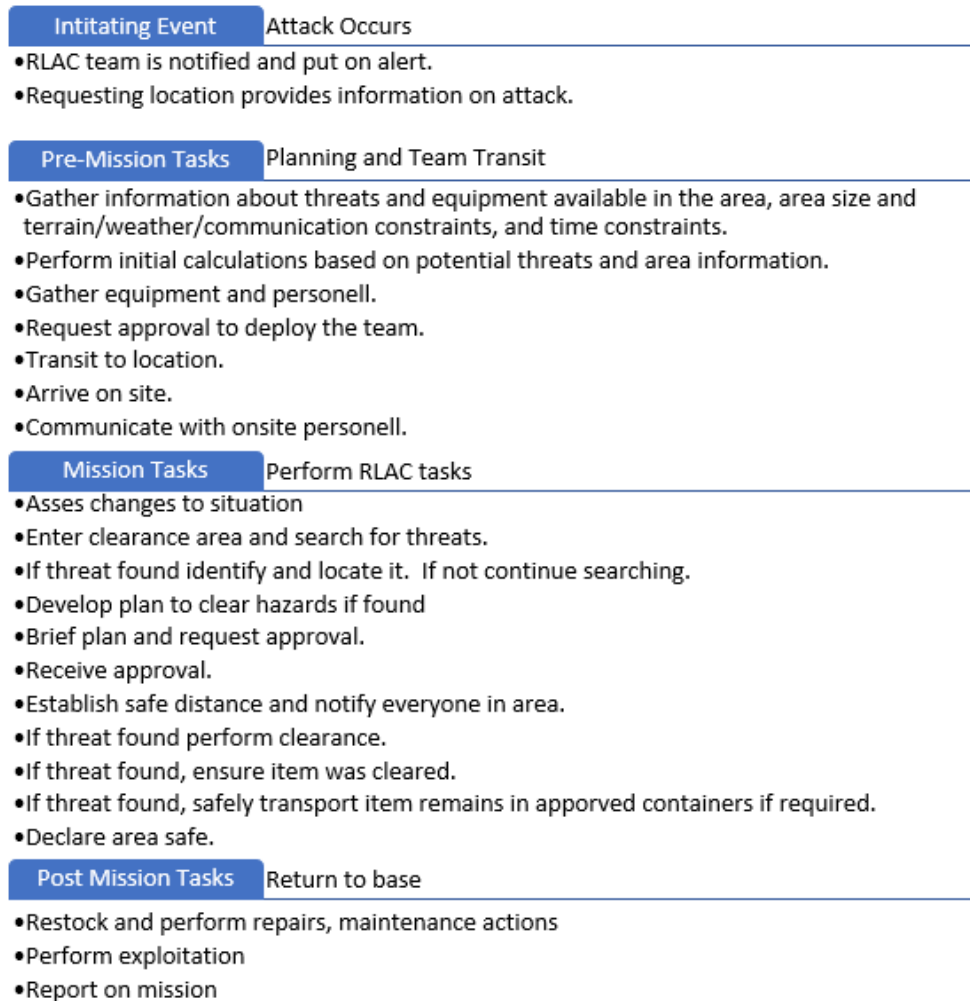


Figure 44. RLAC Concept of Operations

6. Defining Interactions of System

The next step moved into the review existing and developing technology process block as shown in Figure 26. As seen from Figure 42, there were several parts to the RLAC mission. It began with the initiating event and the pre-mission tasks. In general, these were outside of the scope of the RLAC system. They were items that would enable or be required to operate with the RLAC system. The same applied to the post mission tasks. Where the RLAC system fell was in the Mission Tasks. It would be required to be used by an operator to perform some or all of the tasks listed. It may be used in conjunction with the systems from Figure 37.

7. Identifying Constraints

Staying within the process in Figure 26, the next step was to identify constraints. In addition to the constraints shown in Figure 43, several other constraints were listed during the development of the CONOPS. They were shown in Table 11.

Table 11. RLAC System Constraints

Constraint	Type
Must receive permission to perform clearance operations.	Mission/System
Must notify all personnel in area before entering area or taking action.	Mission/System
Must ensure all explosive materials are kept safe and are approved.	Mission/System
No operations during nearby thunderstorms.	Mission
No operations during adverse wind conditions.	Mission
Time limit on operations for sleep/personnel requirements.	Mission

The constraints in Table 11 that were found during CONOPS development were added to the Innoslate model as mission constraints. It could be seen from the generation of the CONOPS that several constraints were added, and the boundary of the system was better aligned with the overall mission. This supported the work performed by Edson and Frittman (Edson, Robert and Frittman 2010).

8. Developing Stakeholder Requirements

Development of the IPCL was skipped as it was outside the scope of developing requirements for RLAC. Instead, the process jumped to the generate requirements documents step, produce draft Enclosure F Requirements Memoranda as shown in Figure 29. Since the CONOPS and stakeholder needs had just been developed the next step was to develop stakeholder requirements.

Once the CONOPS and constraints were developed and identified, the stakeholder needs were turned into stakeholder requirements that took into consideration the CONOPS

and additional constraints. The constraints were mapped to requirements first as these were items that had to be requirements. In instances where there was a mission constraint that did not necessarily have to be a system constraint from Table 11, the requirement indicated that if the system was used under the given conditions, it could not violate the resulting mission constraints. These were areas that could be considered for tradeoffs in system functionality to eliminate mission constraints. Next, the RLAC functions from Figure 42 were turned into requirements.

The requirements were compared to Figure 7 to ensure that all the requirements' areas were covered. From Figure 45 it was seen that most areas had some representation based on stakeholder needs and constraints. The areas that did not have any requirement or had very few were: usability, operational, modes and states, adaptability, design constraints, logistical, and policies and regulations.

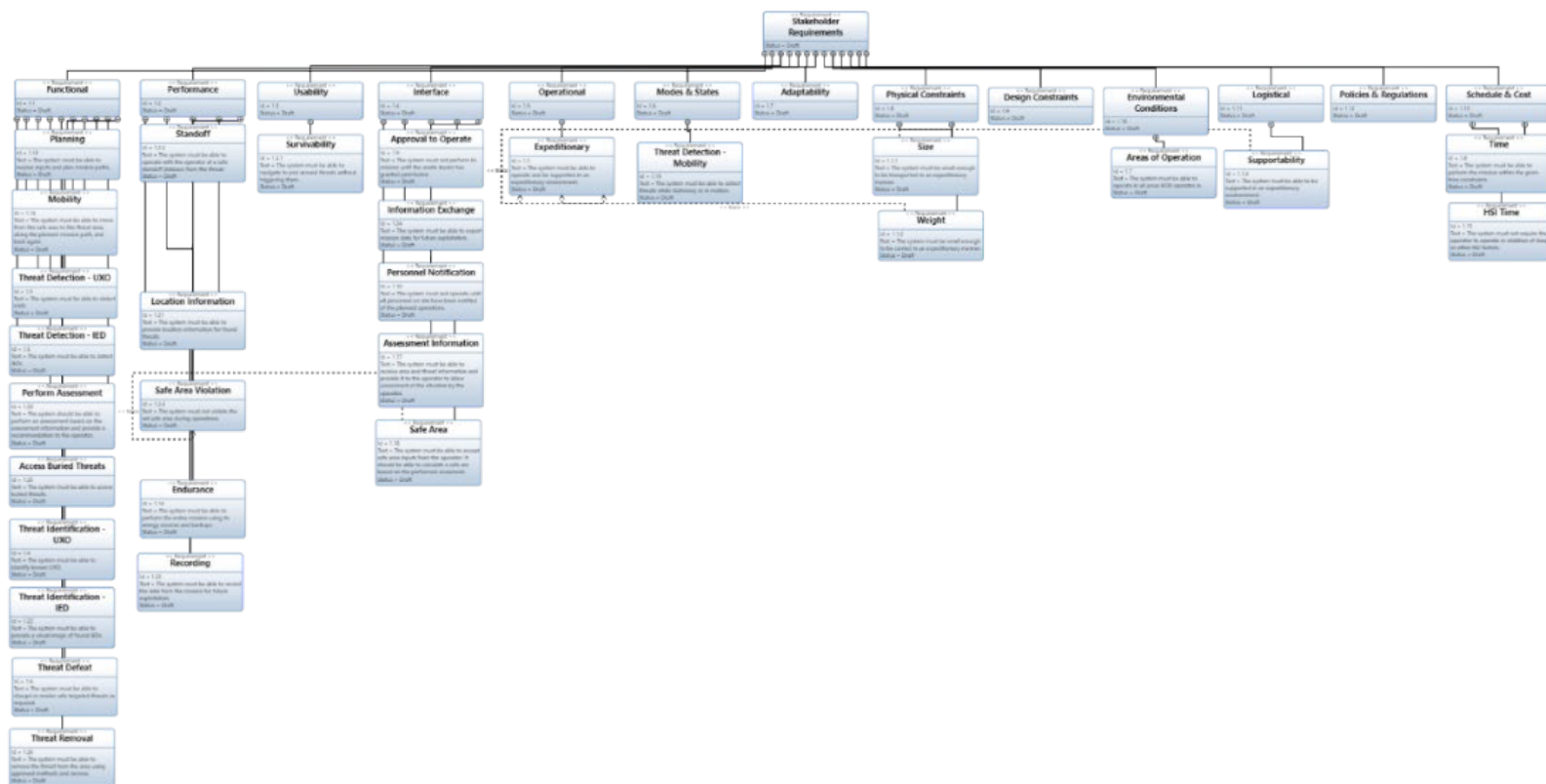


Figure 45. RLAC Stakeholder Requirement Types

Based on this, these areas would need further discussion with stakeholders to ensure there were no missing requirements. This comparison showed that the process did indeed catch potential missing requirements.

9. Defining RLAC Measures of Effectiveness and Measures of Suitability

Staying within the process shown in Figure 29, MOEs and MOSs were developed. From Figure 45, it was seen that the major functional requirements for the system were the ability to receive and transmit information in order to plan and execute missions to detect, identify, assess, access, defeat, and remove threats from an area in an expeditionary manner while keeping the operator safe. This was similar to the stakeholder needs statement of, “The ability to develop, field, and support a system that can be used in expeditionary EOD environments to rapidly clear a large area of hazards while minimizing risks to the operator.” What was missing was the language pertaining to the development and fielding as those requirements were captured under the process requirements. What was added to the statement was the requirements pertaining to the ability to receive and transmit information in order to plan and assess the situation. Based on this, the stakeholder’s needs statement was revised to, “The ability to develop, field and support a system while the threats are still relevant that can be used in an expeditionary EOD environment to rapidly clear a large area of hazards while minimizing risks and operational burden to the operator.”

Based on the overall need statement, the first MOE was that the system must be able to search a large area for threats and provide a negative threat response or the location of threats found within the mission timeframe while allowing the operator to remain at a safe distance. The first MOE would allow the operator to perform the first part of the mission quickly and from a safe standoff distance.

The next MOE was that the system must be able to provide information to the operator that allows the operator to identify the found threats within the mission timeframe while remaining at a safe distance. The second MOE would provide the operator with the information on what the threat was in order to allow them or the system to generate a plan to clear the threats. At this point the remaining MOEs may or may not apply depending on

if threats were found and what type of threat they were. Therefore, the first two MOEs were the most critical and aligned with the prioritized stakeholder needs.

The third MOE was that the system must be able to access any found threats the were buried within the mission timeframe while allowing the operator to remain as safe as possible. Unlike MOE one and two, the operator was not required to remain at a safe standoff distance.

The fourth MOE was that the system must be able to neutralize, render safe, or disrupt any found threats within the mission timeframe while allowing the operator to remain as safe as possible. Like MOE three safe standoff was desired but not required.

The fifth MOE was that the system must remove any found threats from the area in an approved manner. At this point the threat was deemed safe to handle and the area was clear so neither time nor standoff was a factor.

Since all of the above MOEs were threat related, the first MOS was that the system must be able to be adaptable to changing threats so that it is able to be developed and fielded while the threat it is designed to address is still relevant. If this did not occur than even if the system effectively performed the MOEs it would not be suitable for the threats it encountered.

The second MOS was that the system must be able to be operated and supported in an expeditionary environment within the standard EOD mission. If it could not be used in an EOD expeditionary environment than it would not be able to be fielded and supported.

10. Analyzing Stakeholder Requirements

Each of the stakeholder requirements was analyzed to determine if it tied back to a stakeholder need. A traceability matrix was produced and was shown in Appendix A, Figures 60 and 61. All requirements were traced to at least one stakeholder need. The requirements that were traced to 5 or more stakeholder needs were planning, mobility, performance assessment, standoff, expeditionary, and areas of operation. Of these expeditionary and areas of operation had the most traces to stakeholder needs. This implied

that these were the requirements were that were going to need the most breakdown into further detailed requirements as they linked to a large amount of stakeholder needs.

When the same analysis was done for the stakeholder needs in the opposite direction, the needs that traced to the most requirements were downrange initial inspection, access buried threats, take action for buried threats, energy supply concerns, spares, threat types, soil type, and terrain type. Of these, downrange inspection and type of threats traced to the most requirements. This implied that these were stakeholder needs that were going to be the most complicated to fulfill as they had a large scope of requirements needed to capture them.

In particular the areas where the highly populated requirements and needs intersected were expeditionary downrange initial inspection, and the areas of operation that it would be performed in. These were the requirements that would have the most impact in the mission overall if achieved. These were followed by determine soil and terrain type, access buried threats and take action for buried threats in expeditionary areas of operation while addressing energy and spares concerns. This lined up with earlier results that indicated that the highest priority stakeholder needs were plan the mission, deploy to the site, assess the situation, set the safe area, search for possible threats, return to base, and report on actions taken. It added granularity to these needs by showing that the initial down range inspection, assessing the situation, was the most critical. This would determine the soil and terrain type which were required for later steps.

The constraint of expeditionary missions in all EOD environments was the overarching theme that drove many of the requirements and was a good candidate for trying to achieve repeatability in requirements generation.

Appendix A, Figures 61 and 62 also highlighted that several of the stakeholder needs were items required for the RLAC mission but not necessarily for the RLAC system itself. These were mostly involved in planning for the mission, transiting to the mission location, and coordinating with the onsite personnel. The RLAC system would only be required to meet the stakeholder needs specific to it but may have to interface with these other external systems.

B. SYSTEM REQUIREMENTS ANALYSIS

1. Generating Plan for Defining System Requirements

Since the stakeholder needs were not obtained directly from stakeholders for this effort, the steps of negotiate and confirm them with stakeholders were skipped. The next step was in the Charter RWGs block as shown in Figure 33, define the system requirements. As seen from Appendix A Figures 61 and 62, there were several stakeholder requirements that needed to be broken down into greater detail specific to the system. A systems engineering approach utilizing MBSE was used as the approach for defining the system requirements.

2. Establishing System Boundary and Interaction with External Systems

The first step was to establish the system boundary and interactions with critical systems. This had already been started in Figure 37. In addition, Appendix A Figures 61 and 62 showed several stakeholder needs that were required for the RLAC mission but were not needs to be performed by RLAC itself. Figure 37 was modified to show the RLAC system in regard to the external systems and establish the boundary as shown in Figure 46.

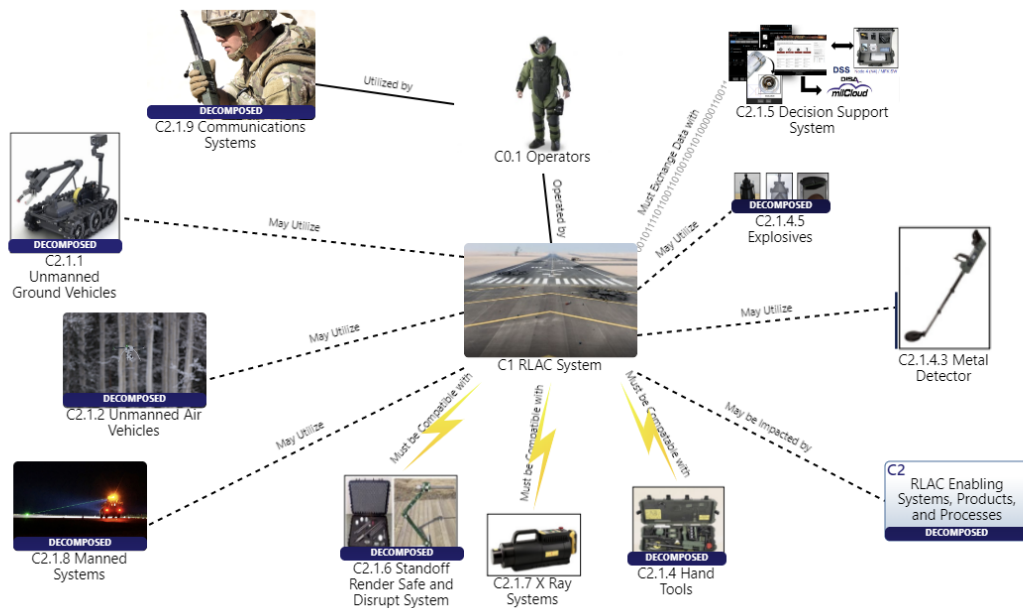


Figure 46. RLAC System Asset Diagram

From Figure 46, it was seen that RLAC had to be able to be operated by operators and had to be compatible with the SRSD system, X-ray systems, and hand tools. It had to be able to exchange data with the DSS system. While not required it may utilize or be interoperable with existing or new unmanned ground vehicles, unmanned air vehicles, manned systems, explosives, and metal detectors. Communications devices used by operators were considered outside the boundary of RLAC and it was not required to interface directly with them. As seen from Figure 46 there was a wide array of equipment that RLAC had to and may have to be interoperable with.

3. Identifying and Defining the Required System Functions

Once the system boundary was determined, the stakeholder requirements and MOEs were used to define the system functions. The stakeholder requirements were first used to define all the functions of the RLAC mission. They were then broken into three major areas. The first was functions that the operator would perform. The second was functions that would be performed by the RLAC system. The functions performed by RLAC were the focus of the analysis. The RLAC functions were arranged in two different ways. One by functional task area and one by functional process area. The functions arranged by task area were shown in Figure 47.



Figure 47. RLAC Functions by Task Area

Figure 47 showed that RLAC had seven main functions by task area which aligned with the steps in the CONOPS and also with the stakeholder requirements. The other way the functions were arranged was by process as shown in Figure 48.



Figure 48. RLAC Functions by Process Area

While Figure 48 showed the functions in a serial order, since they were process' the system would perform, they may not necessarily be performed in that order or in a serial order. Depending on how the system is designed the processes may occur sequentially or in an iterative order or not at all as required by the mission.

4. Proposing a Physical Architecture

Since there were two different ways the RLAC system functions could be arranged, this led to at least two different ways the physical architecture could be defined. When the system functions were looked at from a task perspective, it was seen that there would be six main RLAC systems/subsystems required as shown in Figure 49.

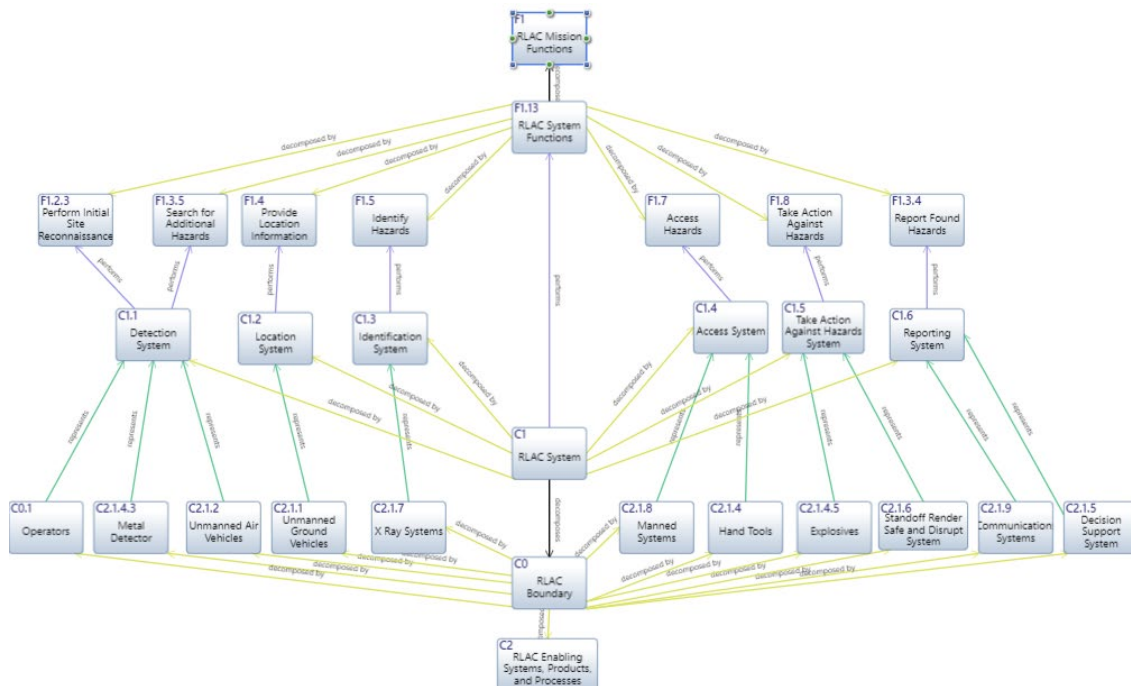


Figure 49. RLAC Physical Architecture by Task Area

Furthermore, from Figure 49 it was seen that each of the six RLAC subcomponents could possibly be performed by existing systems either as is or with modifications.

A similar process was followed for the functions by process which generated Figure 50.

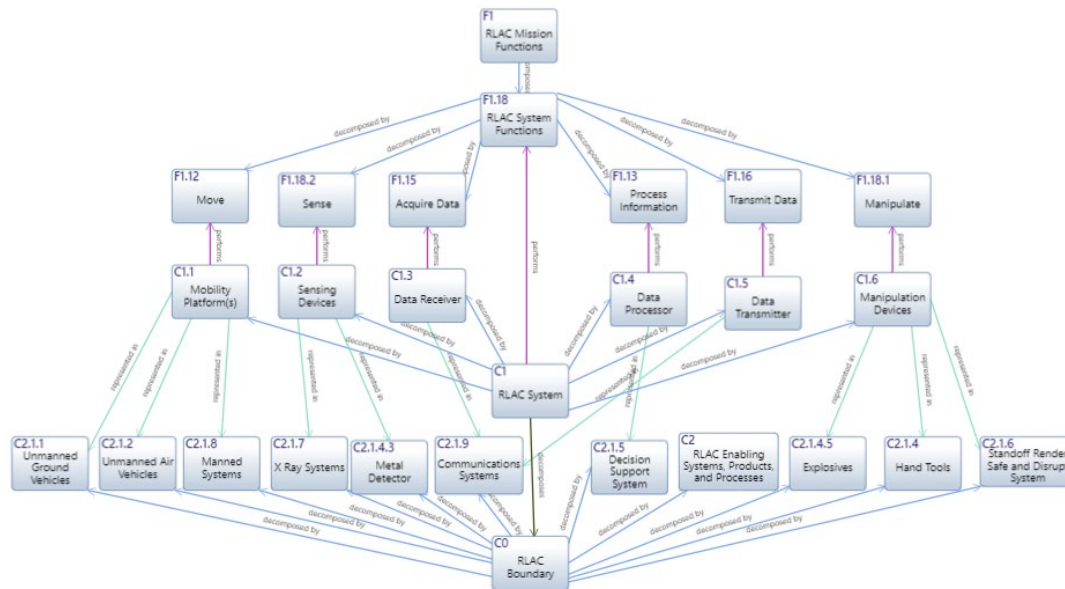


Figure 50. RLAC Physical Architecture by Process Area

When Figure 49 and Figure 50 were compared, two key differences were seen. First, when the functions were aligned by task it appeared that existing system with or without modifications may be able to perform some of the RLAC tasks. Each of the existing systems would have to be compared to the RLAC stakeholder requirements via an AoA to see if this was true or not. If they could, arranging the functions by task would lead to a system of systems that may or may not be interoperable with each other.

When the functions were aligned by process, there was not a one for one line up between the RLAC system components and the existing systems. There were multiple manned and unmanned systems that could be used as a mobility platform. There were a few existing items which could be used as sensing devices. The DSS could be used to process some but not all data. Explosives, hand tools, and the SRSD could be used as

manipulation devices. All of the existing systems would require work to make them interoperable with each other to function together as an RLAC system. The arrangement of functions by process seemed to lead down the path of a single system that performed a wide array of functions or a system of systems that split up some of the functions amongst mobility platforms which would all be required to be interoperable with each other.

5. Identifying Constraints on System

From Figure 43 and Table 11 as well as the stakeholder analysis from Appendix A, Figures 61 and 62, some of the main constraints on the RLAC system were, it had to be expeditionary, able to operate in EOD environments, allow the operator to be remote, and perform the mission quickly. In accordance with the key requirements of the RLAC process and overall JEOD process, the RLAC system also needed to be fielded while the threat was still relevant and not negatively impact of duplicate efforts other services may be working that were similar.

6. Identifying Critical Characteristics

The ability to be expeditionary and able to operate in all areas of EOD operation were ranked higher than the need to be remote or quick and were what were captured as MOSs for the RLAC system. Also, for the stakeholders of the JEOD requirements process to approve the system, it had to be able to be developed and fielded while the threat was still relevant while not duplicating other existing efforts. Due to this, further research was done on existing efforts to determine if their requirements lined up with the RLAC stakeholder needs. Past JEOD requirements and other service requirements were analyzed, and their requirements were put into an Excel spreadsheet that grouped like requirements such as KPPs, time parameters, quantities, effectiveness, accuracy, data, endurance, energy, communications, visual, audio, environmental, human factors, interoperability, reliability, maintainability, availability, transportability, weight, size, survivability, training, cyber, cost, and schedule. The data was not included in the thesis as it was Controlled Unclassified Information (CUI). In general, the existing systems could not accomplish the RLAC stakeholder needs without extensive modifications mostly to address the expeditionary and interoperability requirements.

7. Identifying Technical Risks

While specific RLAC requirements could not be included in this thesis, some generic rapid large area clearance of hazards requirements were modeled in Monterey Phoenix to see how conflicting requirements could cause technical risks, Appendix C Figures 84–90. Similar to the work done in MP for the JEOD process, the root actors were first identified as the team, their equipment, the environment, and the hazard. Basic interactions between each of the actors was then modeled. Due to the number of traces generated, the scope of the program was limited to the detect/locate task only. Only the environments of good or bad weather were looked at and hazards were considered either sensitive or non-sensitive. The only equipment modeled was UAVs, UGVs, and handheld equipment.

When the program was run, it was found that the scenario with the highest likelihood of probability was the equipment was not deployed. This was due to the fact that the UAV could not operate in bad weather and handheld equipment could not be deployed against sensitive hazards due to the requirement to be remote. The next most likely scenario was that the handheld equipment was deployed when there were bad conditions, and the hazard was non-sensitive.

The maximum area scanned occurred when the handheld equipment, UGV, and UAS were deployed simultaneously as shown in Figure 51.

Maximum grids scanned

1. Good weather conditions.
 2. Non-sensitive hazard.
 3. Handheld equipment deploys.
 4. UAV equipment deploys.
 5. UGV equipment deploys.
- Handheld equipment finds 2 hazards (max possible).
 - UAV equipment finds 2 hazards (max possible).
 - UGV does not find any hazards.
 - It took the UGV 10 minutes to search an area and not find anything.
 - If a hazard is found it takes the UGV 20 minutes to scan area.
 - Therefore, if the UGV finds an item it does not have enough time to scan 2 grids. As program requires it to scan 2 grids it was not possible for the UGV to find anything.

Scope 1 – Trace 19

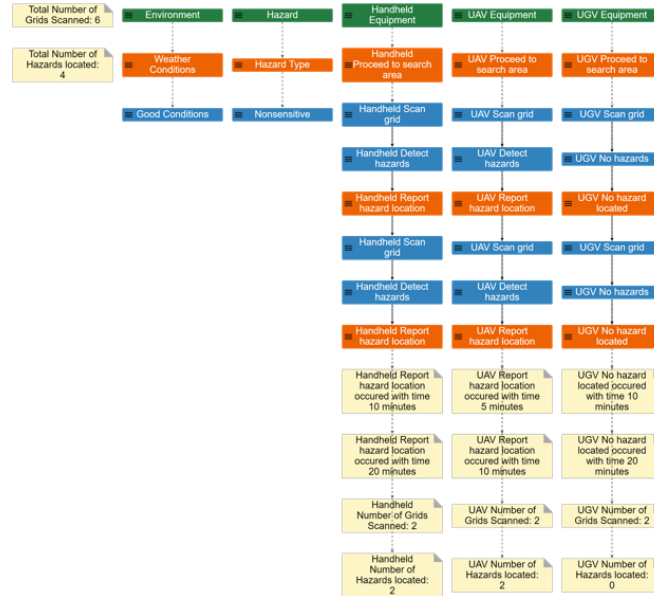


Figure 51. MP Trace for RLAC Maximum Area Scanned

This configuration was able to scan the maximum area as the UAV was fastest at scanning followed by the handheld equipment. They were both able to find all the hazards in their areas. The UGV performed scanning slowly, so it did not have time to scan all of its area and find hazards.

The configuration that found the most hazards was similar with all three items being deployed, but in this case the UGV found its hazard at the start of its scan as shown in Figure 52. The UGV did not have time to scan the rest of the area and find the second hazard.

Maximum Hazards Found

1. Good weather conditions.
2. Non-Sensitive hazard.
3. Handheld equipment deploys.
4. UAV equipment deploys.
5. UGV equipment deploys.

- Handheld equipment finds 2 hazards (max possible).
- UAV equipment finds 2 hazards (max possible).
- UGV finds 1 hazard.
 - It took the UGV 15 minutes to search to find one hazard
 - UGV has a maximum time limit to locate a hazard within 20 minutes.
 - Therefore, if the UGV finds an item it does not have enough time to scan 2 grids.

Scope 1 – Trace 17

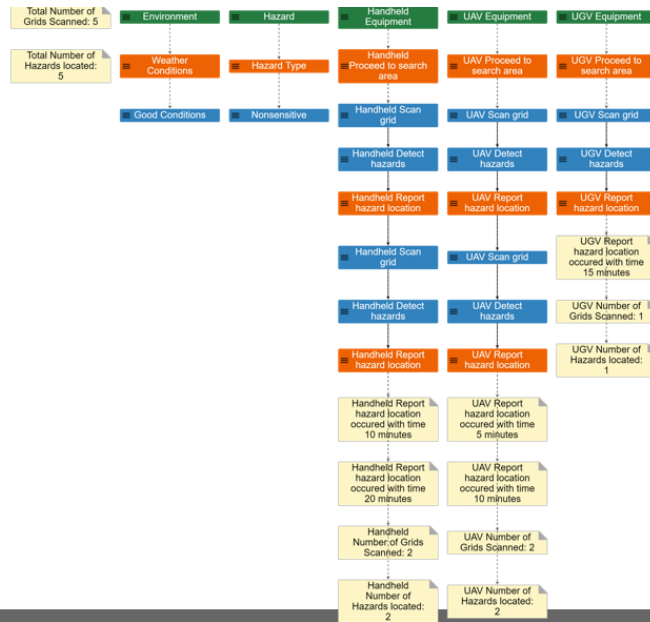


Figure 52. MP Trace RLAC Maximum Hazards Found

The MP program showed that the most efficient solution was to have a kit of systems that could all be deployed together to locate hazards. While the UGV was slowest at locating hazards, it was also the piece of equipment most likely to be able to manipulate a hazard later in the mission if required. While UAVs are fast, they are not able to be deployed in all weather conditions which is a key stakeholder need for the system.

8. Generating System Requirements

This thesis did not go into the generation of system requirements for RLAC. However, based on the stakeholder requirements analysis, the options for physical architecture, the critical features and constraints, and the technology risks a recommendation for overall architecture was proposed.

Since the system had to be fielded while threats were still relevant, the option of going with independent systems aligned by task appeared to be the option that met most of the stakeholder requirements both for the RLAC mission and for the JEOD process. While it would not allow for fully interoperable systems in the near term, it would field something quickly. As the first task of detect and locate was shown by the stakeholder requirements analysis to be the most important task, it should be focused on first for any needed

development. For the time being the systems could remain independent and each have their own CDDs.

As the independent systems are fielded, data should be gathered on their performance to generate an ICD that develops a system of systems which are interoperable and follow the functional tasks based on process approach. This approach will better meet the stakeholder requirements of expeditionary and rapid.

9. Analyzing System Requirements

While this thesis did not generate RLAC system requirements to analyze, past JEOD efforts requirements were analyzed to determine why certain requirements document did or did not make it through the requirements validation process. They were analyzed to see if there were defined and common reasons why the efforts failed or succeeded. The programs analyzed from JEOD were the DSS, the Future Radiographic System (FRS) which became the Radiographic Imaging System for EOD RISEOD, the Advanced EOD Robotic System (AEODRS), and the sub-surface ordnance and improvised explosive device (IED) Locator (SOIL) tool suit. The Army's Man Transportable Robotic System (MTRS) Increment (Inc) 2 was also analyzed as were the USAF RADAS and Expeditionary Airfield Damage Repair (E-ADR). The USN MEMUUV and MESR programs were also studied.

In general, the requirements documents that led to system fielding contained requirements that were traced back to defined threats and CONOPS. The documents also did not indicate what type of technology should be used just what it should be able to achieve. They also provided threshold and objective values and indicated why the objective was desired but not considered achievable at this time. This left room for trade space and technology growth.

The requirements documents that did not result in fielding did not provide as much rationale for the parameters that could be linked back to threats and CONOPS. In the case of AEODRS and MTRS Inc 2 which were similar systems being developed at the same time, the MTRS Inc 2 document specified a very clear reason for the system tied to a specific capability gap and went into detail for all the requirements on how they tied back

to closing that gap. The AEODRS document focused more on technology improvements to allow for open architecture and capabilities beyond what existing systems could already do. However, the AEODRS would still be used for the same gap that existing systems already filled. Due to some of the technology improvements being hard to achieve with limited trade space in the requirements, the AEODRS program was delayed and eventually cancelled when the services shifted their procurement funds to the Army MTRS Inc 2 program.

Even though the MTRS Inc 2 did not meet all the requirements JEOD specified they needed for AEODRS, it did meet several of the requirements discussed in Ch III that were important to the primary stakeholders in the requirements approval process. This reiterated what the analysis in this chapter showed which was that the process must consider the requirements not just of the stakeholders using the system but also of those involved in its procurement. Also, the requirements documents should tie back to threats and CONOPS, which was a recurring theme in the analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. SUMMARY OF RESULTS

This thesis is intended to support the JEOD program by improving the process of requirements generation and by applying this new process to the RLAC mission to begin the development of RLAC requirements by identifying stakeholder needs and mission scenarios. The thesis approached these goals through four phases of research as shown in Figure 53. The thesis began by examining current systems engineering requirements practices—within the JEOD program in DOD, and in the commercial sector. Next, the thesis developed a new requirements generation process for the JEOD program that leverages MBSE and behavioral modeling methods. This was accomplished by studying the limitations and deficiencies of the current JEOD requirements process and identifying how MBSE approaches and best practices could be applied in the form of a new process. The third phase of this thesis used this new process to analyze the RLAC mission and begin the process of developing RLAC requirements by analyzing stakeholder needs and developing RLAC concepts of operation. The fourth and final phase of the thesis summarized the results, assessed the benefits of a MBSE approach to JEOD systems requirements generation, and evaluated the potential use of this new process to other JEOD mission areas and to DOD programs in general.

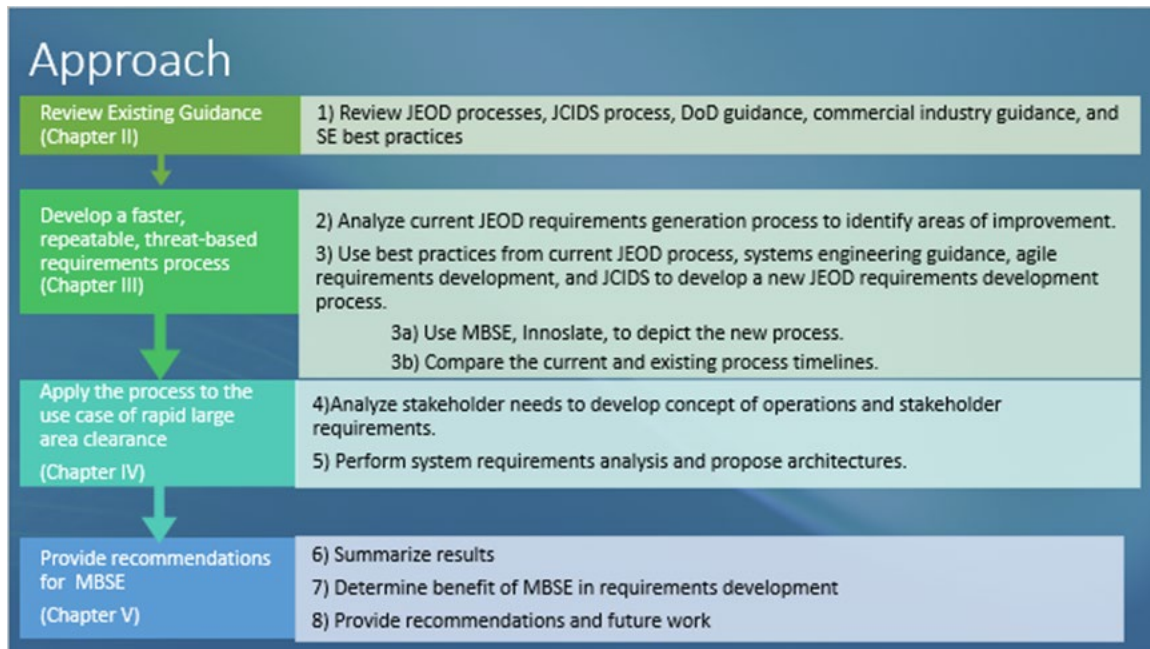


Figure 53. Thesis Steps Taken

The thesis set out to accomplish three objectives. The following subsections restate these objectives and describe how the thesis accomplished them.

1. Objective One Results

The first objective was to develop a requirements generation process for JEOD that could be repeatable with quantifiable threat-based requirements that could be validated through the JCIDS process in a timely manner.

Chapter III showed that the existing process could be modified to be repeatable. Systems engineering and agile principles were used to define new process steps that were inserted into the structure of the existing process. The following items were added to the new process: threat and CONOPS input at various stages as required, alignment of the CDD sections to stakeholder needs, alignment of the CDD sections to DoDAF views, identification of key input and outputs for each step of the process, MBSE artifacts that should be generated or updated for each step of the process, CONOPS that could be used to support industry day and battle lab events, identification of latent stakeholder needs, and definition of MOEs and MOSs. The MBSE diagrams developed in Innoslate that captured

all of these items could be used going forward as a guide for the repeatable process. Additionally, the requirements database that was generated to capture past JEOD and other service requirements could be used to identify repeatable parameters such as environments JEOD operates in.

The process also addressed the objective to have threats as key inputs to the generation of the requirements documents. The process tracked how threats were used throughout the process to generate gaps, scenarios, CONOPS, stakeholder needs, stakeholder requirements, and system requirements. By using MBSE the system requirements could be traced back to the threats and have quantifiable versus qualitative rationales.

Several steps for the generation of the MBSE diagrams, CONOPS, stakeholder needs, and stakeholder requirements were inserted into existing steps of the process versus the charter RWG and write requirements steps. Therefore, the timeline for requirements generation was able to be shortened. While the current process was anticipated to take two years to generate a single validated JCIDS requirements document, the new process could generate one in about a year and a half and two in about two years. This allowed the process to be done in a more efficient manner meeting the last part of the first objective of this thesis.

2. Objective Two Results

The second objective was to apply the new process to the RLAC mission to develop an analytical foundation to support the development of RLAC requirements. The thesis identified common RLAC mission scenarios and stakeholder requirements and assessed the use of the new process to determine its added value to developing system requirements.

The new process was used in an abbreviated format to develop CONOPS and stakeholder requirements. Using the new process confirmed that the stakeholder needs from the overall process were just as critical as those of the stakeholders for the RLAC program. If their needs were not met the program would not succeed. During development of the RLAC stakeholder needs using the new process, it was also confirmed that several of the stakeholder needs were repeatable and tied to sections of the CDD.

The development of CONOPS was also confirmed to be a critical step as their development identified additional constraints and stakeholder requirements. The use of MBSE was able to trace the CONOPS and stakeholder requirements back to stakeholder needs and identify critical stakeholder requirements. This allowed the requirements writer to focus on the critical requirements and ensure that they were properly translated to system requirements.

3. Objective Three Results

The third and final objective was to see if a MBSE approach could add value to the process both in generation of the requirements and in tracking in order to allow future JEOD efforts to have access to the data in a format that can be used to generate other requirements as threats evolve.

MBSE was used extensively in this thesis. The thesis used Innoslate, an MBSE tool to identify process steps along with their inputs and outputs. The tool produced traceability matrices which were also critical to analyzing requirements and developing MOEs and MOSs. The diagrams allowed for easy tracing between the sections of the CDD, what information was required for them, and how they related to the DoDAF views.

The thesis used Monterey Phoenix, a behavioral modeling environment, to demonstrate process flow. In particular, Monterey Phoenix was used to map out a CONOPS and see based on the probability that an actor would perform their step, what would happen overall. This exposed critical process items that were missing such as the CONOPS in the JEOD process generation and over constrained requirements in the RLAC analysis.

B. RECOMMENDATIONS

This thesis has three overall recommendations as described in the following subsections.

1. Recommendation 1 – New Requirements Process Leveraging MBSE

This thesis recommends wide acceptance of this new requirements generation process based on MBSE. The thesis demonstrated the validity of the process through its application to the RLAC mission. The process is repeatable and threat-based; it shortens the time to generate requirements and addresses deficiencies in the current process.

2. Recommendation 2 – JEOD Program Requirements Roles and Tasks

One change that could still be made to improve the process is the constraint on the MTABs time. They were key players in the process but also had other commitments outside requirements generation. The addition of a dedicated requirements writer and a repeatable process would help reduce the burden on the MTABs time. One key area where their burden could be further reduced was in their role to prevent duplication of effort. Instead of the MTAB be the sole provider of requirements their services are working, and the ERB being the sole provider of existing technologies, these tasks could be performed by the requirements writer or the JEOD T and T branch civilians. As the requirements writer was tasked with inserting the information into the documents, they would know what type of information they are looking for. The civilians in the JEOD T and T branch were tasked with providing, “scientific and engineering knowledge and facilities to develop, test, evaluate, and integrate equipment and technologies required to provide joint-military service EOD capabilities” (DOD Directive 5160.62 2021, 8), so this also fits under their mission area.

3. Recommendation 3 – RLAC Approach

In regard to RLAC requirements, the recommendation for development of system requirements is to utilize independent systems that may or may not be interoperable and focus first on the task of detect and locate. This would meet the critical RLAC stakeholder requirements as well as those of the stakeholders of the overall JEOD requirements process (field something in a timely manner without duplication of effort). A longer-term approach would follow the second possible architecture and be a system of systems that was fully interoperable. Lessons learned from the first approach could be incorporated into the second in an incremental approach.

C. FUTURE WORK

Part of the analysis of the current JEOD process indicated a need for a process that could address both deliberate and urgent requirements generation. This thesis focused mainly on the deliberate process. Future work could be done to see how the process could be modified to allow for urgent requirements document generation.

Additionally, the new process was modeled in Innoslate as a process without performers. The process should be broken up to show which stakeholders perform each step and provide data to one another.

While Innoslate was used for this effort, other efforts such as Magic Draw could also be used and additional work could be done to transport MBSE diagrams created in this thesis into Magic Draw.

Excel was currently used to create a requirements database as the data was CUI. This data could be used to generate MBSE models on a secure server which could connect to the RLAC requirements as well as future requirements efforts.

Finally, Monterey Phoenix showed potential as a method to validate overly constrained requirements. It would be interesting to use it to map requirements for existing requirements efforts that succeeded or failed to see if Monterey Phoenix would show any emergent behavior or patterns. The idea of using a program like Monterey Phoenix to enter requirements with their thresholds and objectives, real world feasibility of actors, and see where things do not line up is intriguing. One of the hardest parts of requirements is they can often not be validated until the system is built.

APPENDIX A. INNOSLATE MODELS

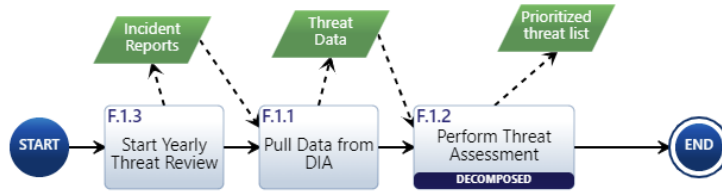


Figure 54. Current Threat Analysis Process

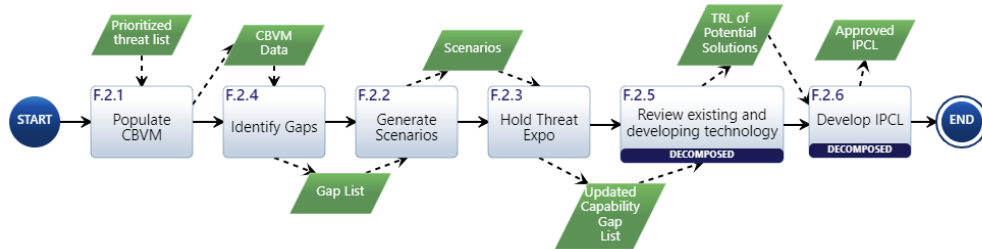


Figure 55. Current Capability Gap Definition Process

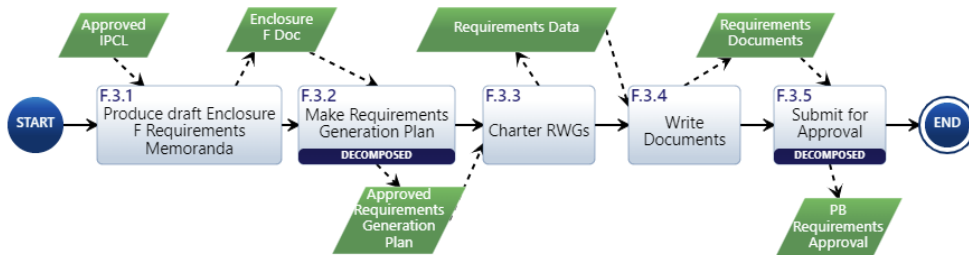


Figure 56. Current Existing Requirements Generation Process

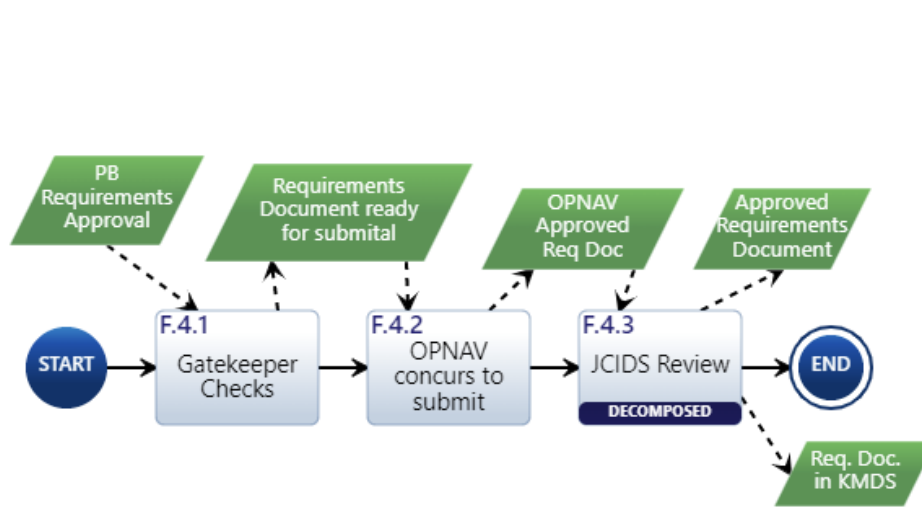


Figure 57. Current JCIDS Validation Process

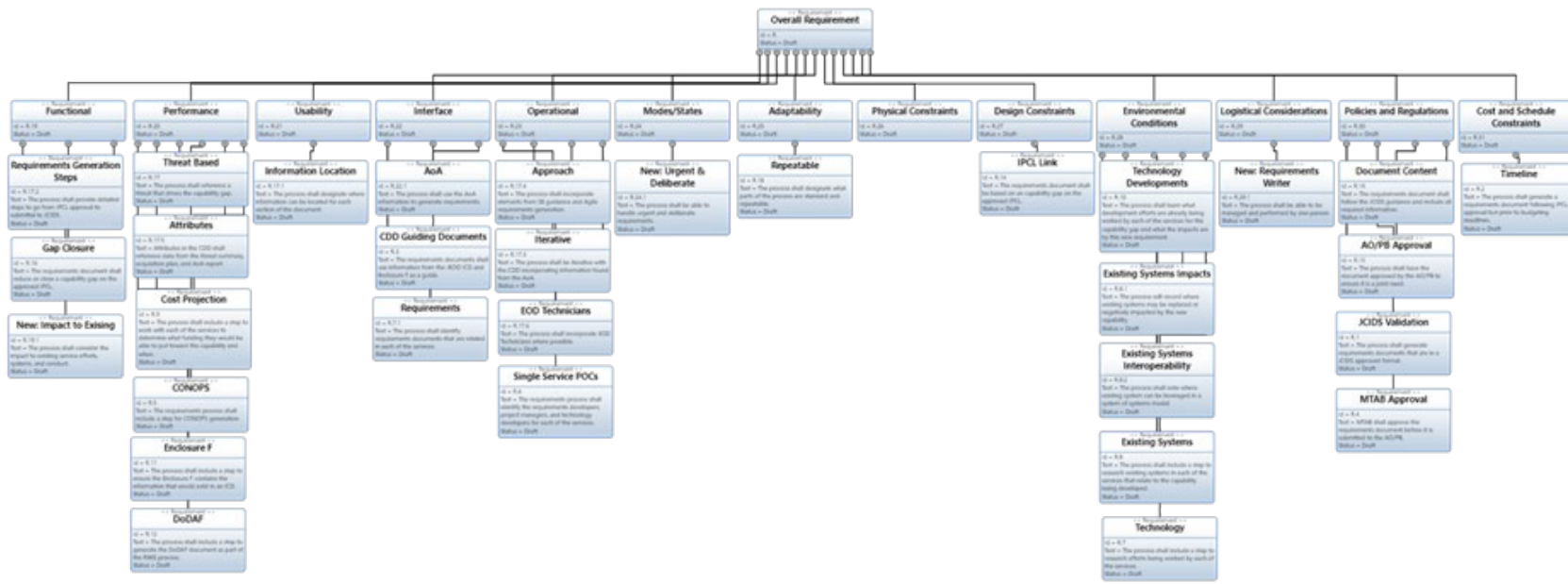


Figure 59. JEOD Process Stakeholder Requirements

Overall Requirement to Related Entities	SN1.1.1 Duplication of Effort - JCIDS Need (S)	SN1.1.2 Competing Efforts - PB Need (L)	SN1.1.3 Enclosure F - MTAB (S)	SN1.1.3 Duplication of Effort - MTAB (S)	SN1.1.4 System Replacement - PMO (L)	SN1.1.5 Requirements Overlap - RD (S)	SN1.2.1 System Effective - JCIDS Need (S)	SN1.2.1 IPCL Connection - PB Need (S)	SN1.2.2 Capability Gap Closure - MTAB (S)	SN1.3.1 Approval for Use - MTAB (L)	SN1.3.2 System Effectiveness - EOD Technicians (S)	SN1.3.3 Document Types - RD (S)	SN1.3.4 JCIDS Validation - RD (S)	SN1.5.1 Service Specific Systems - ERB (S)	SN1.5.2 Service Considerations - RD (S)	SN1.5.3 System Interoperability - RD (S)	SN1.6.1 Budgeting Details (S)	SN1.6.2 Efficient Process - MTAB (L)	SN1.6.3 Threat Relativity - EOD Technicians (L)	SN1.6.4 Acquisition & Support Information - PMO (S)	SN1.6.5 Development Funding - SSTD (L)	SN1.6.6 Development Funding - TD (L)	SN1.7.1 Training - TTAB (S)	SN1.7.2 Training - NAVSCOLEOD (S)	SN1.7.3 Training - EOD Technicians (S)
R.1 JCIDS Validation						X						X													
R.2 Timeline																	X		X		X	X			
R.3 CDD Guiding Documents												X													
R.4 MTAB Approval								X	X																
R.5 CONOPS						X				X															
R.6 Single Service POCs												X						X							
R.7 Technology					X										X						X	X			
R.7.1 Requirements												X						X							
R.8 Existing Systems	X			X								X	X	X											
R.8.1 Existing Systems Impacts													X	X											
R.8.2 Existing Systems Interoperability				X								X	X			X							X	X	X
R.9 Cost Projection																	X								
R.10 Technology Developments		X	X		X							X			X										
R.11 Enclosure F			X																						
R.12 DoDAF													X												
R.13 AO/PB Approval		X																							
R.14 IPCL Link							X																		
R.15 Document Content												X	X												
R.16 Gap Closure						X		X		X									X						
R.17 Threat Based						X													X						
R.17.1 Information Location																		X							
R.17.2 Requirements Generation Steps												X	X					X							
R.17.3 Iterative																									
R.17.4 Approach																									
R.17.5 Attributes																X						X	X	X	
R.17.6 EOD Technicians																									
R.18 Repeatable																	X								
R.19 Functional																									
R.19.1 New: Impact to Existing	X	X		X	X									X	X	X			X						
R.20 Performance																									
R.21 Usability																									
R.22 Interface																									
R.22.1 AoA												X	X												
R.23 Operational																									
R.24 Modes/States																									
R.24.1 New: Urgent & Deliberate																									
R.25 Adaptability																									
R.26 Physical Constraints																									
R.27 Design Constraints																									
R.28 Environmental Conditions																									
R.29 Logistical Considerations																									
R.29.1 New: Requirements Writer																									
R.30 Policies and Regulations																									
R.31 Cost and Schedule Constraints																									

Figure 60. JEOD Process Requirements Traceability Matrix

Figure 61. RLAC Requirements Traceability Part 1

Figure 62. RLAC Requirements Traceability Part 2

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. JEOD AND RLAC DATA

Table 12. JEOD Stakeholder Needs

Stakeholder	Needs	Type
JCIDS	Ensure that the submitted documents were written in a manner that prevented systems from being developed and fielded that were not able to be operationally effective throughout their life cycle.	Stated
	Ensure that the documents did not duplicate efforts already developed or being developed by other sponsors.	Stated
JEOD: Program Board and Action Officers	Requirements documents work to close capability gaps on the IPCL they approved.	Stated
	The documents must contain enough detail to allow each of their services to budget for procurement and support of the systems.	Stated
	The documents must not compete with efforts they may be working for a single service need.	Latent
JEOD: MTAB	Requirement document that they can submit to the AO/PB that can be used to work to close a capability gap.	Stated
	Enough information to generate an Enclosure F and determine if the proposed requirements are unique to JEOD or if they can be filled by an existing single service requirement document.	Stated
	Proper information in the requirements document that can be used during the development process to approve the system for joint service use.	Latent
	A process that is efficient as they are the focal point for requirements generation on behalf of their services.	Latent
JEOD: ERB	Information on equipment their services use and how it relates to the capability gap.	Stated
JEOD: TTAB	Information on how the system will be used in order to provide training requirements.	Stated
JEOD: NAVSCOLEOD	Information on how the system will be used in order to provide training requirements.	Stated
Single Service: EOD Technicians	System that allows them to perform the mission in the most effective way possible mitigating risk as much as possible.	Stated
	Training on the system in order to use it properly.	Stated
	System that is fielded while the threat is still relevant.	Latent

Stakeholder	Needs	Type
Single Service: Program Offices	Information from the requirements process to determine how many systems they would buy based on the capability it will provide, when the systems would be available for procurement, how much they would cost, what the sustainment plans would be and how much they should budget for them.	Stated
	Technical information to determine if the new systems would replace any of their existing systems.	Latent
Single Service: Requirements Developers	Requirements and supporting information in a format that their service will accept.	Stated
	Information to determine if the requirements overlap with any of their existing capability document.	Stated
	Information on how the system will fit into their overall service mission.	Stated
	Need to know if the system will connect to any other systems they use in their service and impact their use.	Stated
	Proper information to generate a requirements document that can be validated in JCIDS.	Stated
Single Service: Technology Developers	A chance to compete for development work.	Latent
Technology Developers	A chance to compete for development work.	Latent

Table 13. JEOD to Product Development Comparison

Current Process Steps	Product Development (Ulrich and Eppinger 2016)
Start yearly threat review	Gather raw data from customers
Pull data from DIA	
Perform threat assessment	
Populate CBVM	Interpret the data
Identify gaps	
Generate scenarios	Organize the needs by type
Hold threat expo	

Current Process Steps	Product Development (Ulrich and Eppinger 2016)
Review existing and developing technologies	
Develop IPCL	Establish priority
Produce Enclosure F Requirements Memorandum	Reflect on the results
Make requirements generation plan	
Charter RWGs	
Write documents	
Submit for approval	
JCIDS validation process	

Table 14. JEOD to Needs and Goals Comparison

Current Process Steps	Needs to Goals (Crawley, Cameron, and Selva 2016)
	Identify stakeholders
Start yearly threat review	Identify needs
Pull data from DIA	
Perform threat assessment	
Populate CBVM	Group stakeholders
Identify gaps	Characterize needs
Generate scenarios	Stakeholders as a system
Hold threat expo	
Review existing and developing technologies	
Develop IPCL	Prioritize needs
Produce Enclosure F Requirements Memorandum	Map needs to goals
	Criteria for goals
Make requirements generation plan	Prioritize goals
Charter RWGs	Formulate goals

Current Process Steps	Needs to Goals (Crawley, Cameron, and Selva 2016)
Write documents	Develop metrics
Submit for approval	
JCIDS validation process	Check that goals met key needs

Table 15. JEOD to INCOSE Comparison

Current Process Steps	INCOSE (Walden et al. 2015)
Start yearly threat review	
Pull data from DIA	2 - Identify enabling systems, products, or services
Perform threat assessment	
Populate CBVM	
Identify gaps	3 - Gather stakeholder needs
Generate scenarios	5 - Develop Operational scenarios
Hold threat expo	6 - Define interactions of system
Review existing and developing technologies	7 - Identify constraints
Develop IPCL	4 - Prioritize stakeholder needs
Produce Enclosure F Requirements Memorandum	8 - Develop stakeholder requirements
	9 - Define measures of effectiveness (MOEs) and measures of suitability (MOSs)
Make requirements generation plan	10 - Analyze requirements
	11 - Negotiate modifications for unrealizable or impractical requirements
	12 - Confirm requirements with stakeholders
	13 - Record requirements in a database
Charter RWGs	1 - Identify Stakeholders
	1 - Establish approach for defining system requirements
	2 - Establish system boundary and determine interaction with external systems
	3 - Identify and define the required system functions

Current Process Steps	INCOSE (Walden et al. 2015)
	4 - Identify constraints on system from stakeholder requirements or organizational limitations
	5 - Identify critical characteristics such as safety, security, reliability, and supportability.
	6 - Identify technical risks
Write documents	7 - Specify system requirements. May use documentation tree to establish hierarchy. Capture rational for each requirement.
	8 - Analyze requirements
	11 - Define verification criteria such as measures of performance (MOPs) and technical performance measures (TPMs) which should trace to MOEs and MOSs
Submit for approval	9 - Present requirements to stakeholder to ensure they agree
	10 - Negotiate modifications
	12 - Ensure stakeholders agree
JCIDS validation process	13 - Establish traceability
	14 - Record requirements in a database

Table 16. JEOD to DOD SE Comparison

Current Process Steps	DOD SE Model (DAU 2014)
Start yearly threat review	Stakeholder Requirements Definition
Pull data from DIA	
Perform threat assessment	
Populate CBVM	
Identify gaps	
Generate scenarios	
Hold threat expo	
Review existing and developing technologies	
Develop IPCL	
Produce Enclosure F Requirements Memorandum	
Make requirements generation plan	Requirements Analysis

Current Process Steps	DOD SE Model (DAU 2014)
Charter RWGs	
Write documents	Design
Submit for approval	
JCIDS validation process	Product

Table 17. JEOD to Agile Comparison

Current Process Steps	Agile (Kitowska 2022)
Start yearly threat review	Define Epic user need
Pull data from DIA	
Perform threat assessment	
Populate CBVM	
Identify gaps	Breakout stories under the Epic
Generate scenarios	
Hold threat expo	
Review existing and developing technologies	
Develop IPCL	
Produce Enclosure F Requirements Memorandum	Create a card for each story. Stakeholder, requirement, acceptance criteria.
Make requirements generation plan	
Charter RWGs	Create tasks for each story
Write documents	
Submit for approval	
JCIDS validation process	

Table 18. Current JEOD Process Constraints

Constraint	Type	Stakeholder Need Affected
One of the services requires a CDD for procurement. Middle Tier Requirements Documents such as a (TLR) cannot be used.	Hard	Required Documents (4)
CDDs must go through the JCIDS process.	Hard	Required Documents (4)
CDDs require AoAs and DODAF documents.	Hard	Required Documents (4)
MTAB must submit an Enclosure F to start the CDD generation.	Soft	Required Documents (4)
Requirements documents must tie to an item on the approved IPCL.	Soft	System Effective (1)
Documents must be approved by multiple entities.	Hard	System Effective (1)
MTAB represents interests of EOD Technicians.	Soft	System Effective (1)
At least two services must require the capability for it to be considered joint.	Hard	Duplication of Effort (2)
Requirement cannot overlap with existing systems or requirements services may be working.	Hard	Duplication of Effort (2)
Threat Analysis occurs yearly.	Soft	Schedule (3)
Budgeting cycle occurs yearly.	Hard	Schedule (3)
Requirement must consider 4 services when looking at interoperability.	Hard	Interoperability (5)
JEOD requirements development funding for 1 requirements writer.	Soft	Budget (6)
MTAB responsible for assisting with requirements development.	Soft	Budget (6)
Aside from MTAB other stakeholders not required to participate in RWGs.	Hard	Budget (6)

Table 19. JCIDS DoDAF Connections

View	Required For	JCIDS Links	DoDAF Links	Notes (DoDAF 2010)
AV-1: Overview and Summary Information	All			
OV-1: High-Level Operational View	All	Section 1: Operational Context	OV-2	Highest level of concept of CONOPS. Ensure interoperability is displayed at a high-level.

View	Required For	JCIDS Links	DoDAF Links	Notes (DoDAF 2010)
OV-2: Operational Resource Flow	All	Section 1: Operational Context Section 7: Interoperability	OV-1 OV-4 OV-5a SV-1 SV-2 SV-8	Translates OV-1 to show connections between the system(s) and operator(s) that are required to execute the mission. The OV-2 should line up with the joint physical interoperability discussed in this section. Should discuss resource flows to and from capability. Should also link to SV-1. Show SoS or FoS. Show any future increment capabilities. Complemented by SV-1 and SV-2. Used to show if net ready certification is required or not.
OV-3: Operational Resource Flow Matrix	All	Section 7: Interoperability		Lists resources exchanged and how they are exchanged. Include Net ready interoperability table if applicable.
OV-4: Organizational Relationships Chart	All	Section 1: Operational Context Section 4: Program Summary Section 9: Intelligence Support	OV-2 OV-5a OV-5b StdV-1	Overview of organizations involved in CONOPS. The OV-4 should include and line up with anyone using the system as discussed in section 4. Intelligence Interoperability addresses exchange of information and intelligence with an organization outside of the Service developing the capability. Must be defined requirements at the data, tool, process and organization levels. Data standards, activities and organizational relationships must be documented in StdV-1, OV-4, OV-5b according to App H to Enc B.

View	Required For	JCIDS Links	DoDAF Links	Notes (DoDAF 2010)
OV-5a: Operational Activity Decomposition Tree	All	Section 1: Operational Context Section 7: Interoperability	CV-2 CV-3 CV-6 SV-5a	Hierarchy to show capabilities and operational activities. Shows relationship between OV-2 and associated UJT. Provides traceability between other views and JCIDS documents back to UJT.
OV-5b: Operational Activity Model		Section 7: Interoperability	OV-4 OV-5b SV-5a StdV-1	Connections between items in OV-5a. Inputs/outputs/performers, etc. Intelligence Interoperability looks at information exchanged with an organization outside of the Service developing the capability. Must be defined requirements at the data, tool, process and organization levels. Data standards, activities and organizational relationships must be documented in StdV-1, OV-4, OV-5b according to App H to Enc B.
OV-6a: Operational Rules Model				Used to describe how the organization functions. Identifies business rules that are constraints.
OV-6b: State Transition Description				Used to describe how the organization functions. Identifies processes that occur due to events.
OV-6c: Event Trace Description	All, minus SW-ICD			Used to describe how an organization functions. Traces actions in the process or scenarios.
CV-1: Vision	All, minus SW-ICD			Defines the strategic vision for the capabilities. Addresses context and concerns with how the new capabilities will fit into overall organization vision.

View	Required For	JCIDS Links	DoDAF Links	Notes (DoDAF 2010)
CV-2: Capability Taxonomy	All, minus SW-ICD	Section 3: Capability Discussion - CDD Table: CDD Capability Requirement to Performance Attribute Traceability Section 4: Program Summary Section 5: Performance	OV-5a CV-3 CV-6	Presents hierarchy of capabilities. Can be in context of a timeline. Current and future. Must be consistent with operational attributes in Annex A of Appendix B. Must be expressed in terms of operational effectiveness rather than performance of a presumed solution. Quantitative criteria for mission success must be established for each capability. Must be consistent with planned program activities.
CV-3: Capability Phasing	All, minus SW-ICD	Section 3: Capability Discussion - CDD Table: CDD Capability Requirement to Performance Attribute Traceability Section 4: Program Summary Section 5: Performance	OV-5a CV-2 SV-7	The planned achievement of capability at different points in time or during relevant periods of time. Builds on CV-2. Can be used to show incremental approach. Shows when capabilities introduced and how they fit into overall plan. Shows functions, conditions, desired results, constraints, resources, and acceptance criteria for the capabilities. Feeds SV-7. IOC and FOC timeframes must be consistent with CV-3. Parameters must be consistent with CV-3.
CV-4: Capability Dependencies				Shows dependencies between each of the capabilities.
CV-5: Capability to Organizational Development Mapping				Shows capability, performers, their environment, their concepts of employment for the capability and how it is used in each phase.

View	Required For	JCIDS Links	DoDAF Links	Notes (DoDAF 2010)
CV-6: Capability to Operational Activities Mapping	All, minus SW-ICD	Section 3: Capability Discussion - CDD Table: CDD Capability Requirement to Performance Attribute Traceability	OV-5a CV-2	Shows connections between required capabilities and the operational capabilities that they support. Shows traceability between the capabilities in CV-2 and the operational activities in the OV-5a.
CV-7: Capability to Services Mapping				Shows connections between capabilities and the functions they enable.
SV-1: Systems Interface Description	CDD, IS-CDD	Section 7: Interoperability Net Ready Table	OV-2	Identification of connections between systems and subsystems. Shows what triggers the process in the OV-2 now or in the future. Shows any physical requirements that may impact the joint force or any SoS or FoS considerations. Shows what network the system must connect to. If NR certification not applicable SV-1 must be included to support the decision.
SV-2: Systems Resource Flow Description	CDD, IS-CDD	Section 7: Interoperability Net Ready Table	OV-2	Shows resources exchanged between systems. Shows what network the system must connect to. If NR certification not applicable SV-2 must be included to support the decision.
SV-3: Systems-Systems Matrix				Shows relationships among systems in the chosen design.
SV-4: System Functionality Description				Shows the functions performed by systems. Along with the data flow that may exist between system functions.

View	Required For	JCIDS Links	DoDAF Links	Notes (DoDAF 2010)
SV-5a: Operational Activity Systems Function Traceability Matrix to			OV-5a OV-5b	Shows how system functions connect to operational activities.
SV-5b: Operational Activity Systems Traceability Matrix to				Shows how systems link back to capabilities or operational activities.
SV-6: Systems Resource Flow Matrix		Section 7: Interoperability Net Ready Table		Shows resources shared between systems. Shows how they are exchanged. Shows time to connect and/or how system is managed on the network. Shows the information exchanged and how it is exchanged.
SV-7: Systems Measures Matrix	CDD, IS-CDD	Section 5: Performance Section 7: Interoperability Net Ready Table	SV-8	Shows the ways in which system will be measured. Include the appropriate timeframe. Shows connection to other DoDAF views. Discussion of capability dependencies must be consistent with SV-8. Must show all external dependencies.
SV-8: Systems Evolution Description	CDD, IS-CDD	Section 3: Capability Discussion Section 5: Performance		Shows the plan for incremental development of a suite of systems or increases in performance over time.

View	Required For	JCIDS Links	DoDAF Links	Notes (DoDAF 2010)
SV-9: Systems Technology and Skills Forecast				Shows emerging technologies and skills that may affect future system development.
SV-10a: Systems Rules Model				Describes system functionality. Identifies design and implementation limitations that may affect the systems functionality.
SV-10b: Systems State Transition Data				Describes system functionality. Identifies how the system responds to events.
SV-10c: Systems Event Trace Description				Describes system functionality. Highlights events in OVs that are critical to system functioning.

Table 20. RLAC Stakeholder Needs

Stakeholder	Stakeholder Need
JEOD Program Board and Action Officers	RLAC requirement document(s) that will be acceptable to each of the services they represent and will not result in duplication of program/budgeting effort.
MTAB	Requirement document that they can submit to the AO/PB that can be used to work to meet the RLAC needs.
	RLAC solution that they can approve for use that each of their services will find acceptable and effective.
	Enough information to determine if the proposed requirements are unique to JEOD or if they can be filled by an existing single service requirement document.
TTAB	Enough information to approve training on the RLAC system.
ERB	Prototypes to test to ensure they will perform the RLAC mission in the operational environment.
	Enough information to provide to the MTAB to grant an approval for use: performance, safety, cyber, EMI, etc.

Stakeholder	Stakeholder Need
EOD Technicians	Determine if there are any explosive hazards in an area.
	Determine where explosives are at in an area.
	Provide data to allow the technician/system to go to the explosives location without coming near any other explosives in the area.
	Provide information to allow the technician to determine what type of explosive hazard it is.
	If the item is buried and needs to be dealt with, provide a way to get to it to neutralize, render safe, or disrupt it.
	Neutralize, render safe, or disrupt the threat based on what kind it is.
	If the threat has to be removed from the area, provide a way to safely move it.
	Perform the mission in an expeditionary manner. Small teams. Small equipment size.
	Be able to perform the mission in all environments JEOD operates in but particularly on large areas such as runways, roadways, and Forward Operating Bases (FOB)s.
	Be able to perform the mission rapidly. Would like to have the area declared safe to enter within x hours.
	Would like to be able to perform all tasks remotely until the threat is located and known to be safe to be near.
	If there is a need to approach an unsafe item, need equipment to approach while mitigating risk to technician.
	System needs to be able to last long enough to complete an x hour mission.
	Energy supplies need to be able to work in remote areas and use existing equipment to recharge/resupply in those environments.
	System needs to have spares as mission will be performed in remote areas without access to repair equipment. But weight and size are a concern.
	System needs to be able to be transported to remote areas in vehicles and helicopters that are limited on space for equipment.

Stakeholder	Stakeholder Need
	System will need to be able to be operated by only x people at a time preferably only x.
	System will need to be able to operate in comms degraded/denied areas.
	System will need to operate in areas that may be contaminated with chem/nuclear/bio.
	System will need to be able to work on explosive threats that EOD encounters such as but not limited to IEDs and UXO. The system may encounter UXO that employ chem and bio.
Single Service EOD Program Offices (outside NAVSEA 05)	When will the system be available for procurement so we can budget for it.
	How much will the system cost. Needs to be affordable.
	What type of capability will it deliver.
	What type of support will it require.
	Is it planned to replace any existing equipment.
Single Service Requirements Developers	Does the capability overlap with any of our existing capability documents.
	How does the proposed capability connect to other systems we use.
	Will the capability as defined meet our single service requirements. Need to consider how EOD mission fits into overall service mission.
	Is the document in the right format to get approval through our single service requirements process.
Single Service and Industry/Academia Technology Developers	Are we working on anything that can fill this capability gap? Is there an opportunity for us to work on something.
	What is the schedule/funding available to work on development.
Navy School EOD	Information to develop training for the new system.

Stakeholder	Stakeholder Need
	Systems to use while developing training.
	Any user guides or manuals that go with the system.
EOD T and T	Requirements documents that provide the information needed to develop and test a new system.
	Information to develop new/updates to procedures and publications.
Resource Sponsor	Statement of Need from JEOD describing the RLAC capability gap to start resourcing.
	Information to generate a requirements document.
Project Manager – NAVSEA 05	Validated Statement of Need from Resource Sponsor to begin work.
	Requirements documents that provide the information needed to develop an acquisition plan.
	Information to perform an AoA if required.

APPENDIX C. MONTEREY PHOENIX CODE AND RESULTS

```

Run Scope: 1
1 /* Model of Joint Service Explosive Ordnance Disposal (JSEOD) Capability Development Document (CDD) process
2 Created by Angel Gill Dec 2021
3
4 Purpose: Map interactions in JSEOD required to develop CDD.
5 Determine failure and critical points in process.
6
7 Description: This model will map out the people and tasks required to write a CDD.
8 It will show how the tasks are connected. It will begin with a requirements working
9 group being developed.
10 It will end with a completed CDD ready to be submitted to OPNAV for the
11 Joint Capabilities Integration Development System (JCIDS) process.
12
13
14 References:
15 (1) JSEOD Section F SoN process.
16 (2) JCIDS Manuel 2018 Version
17 (3) Model of Supply Chain with Two Cyber Threats
18 Based on the "Baseline Supply Chain" model
19 Created by Nathaniel Alden with help from Rachel Talkington on the 5th of July, 2020.
20
21
22 Search terms: Capabilities Development Document, CDD, JCIDS, Requirements
23
24
25

```

Figure 63. Lines 1–25: Title, Description, References

```

26 =====*/
27 SCHEMA JSEOD_CDD /*Joint Service Explosive Ordnance Disposal
28 Capabilities Development Document.*/
29
30 /*Key actors in the CDD process are shown below with their tasks.*/
31
32 /*Military Technical Acceptance Board Actions.
33 MTAB is composed of 1 member from each of the 4 services.
34 They all must provide approval. Modeled here as 1 unit.
35 They can either provide the requested data or not provide the data.*/
36 ROOT MTAB: { * <1> MTAB_Members * };
37     MTAB_Members:
38         (Provide_CONOPS | Do_Not_Provide_CONOPS) /*Include fielding data.*/
39         (Provide_Related_Work_Data | Do_Not_Provide_Related_Work_Data) /*Includes requirements.*/
40 ;
41
42 /*Threat Subject Matter Expert Actions. Expert on threats that JSEOD faces.
43 They can either provide the requested data or not provide the data.*/
44 ROOT Threat_SME: (Analyze_Threats
45     (Provide_Threat_Data | Do_Not_Provide_Threat_Data)
46     | (Do_Not_Analyze_Threats | Do_Not_Provide_Threat_Data)
47 )
48 ;
49
50 /*Data that they must have to complete their actions. */
51 COORDINATE $a: Provide_CONOPS FROM MTAB,
52             $b: Analyze_Threats FROM Threat_SME
53             DO ADD $a PRECEDES $b;
54             OD;
55
56 COORDINATE $a: Do_Not_Provide_CONOPS FROM MTAB,
57             $b: Do_Not_Analyze_Threats FROM Threat_SME
58             DO ADD $a PRECEDES $b;
59             OD;
60
61

```

Figure 64. Lines 26–61: SCHEMA, ROOTS MTAB and Threat SME

```

62 /*Project Management Office Actions.
63 They can either provide the requested data or not provide the data.*/
64 ROOT PM: {(Develop_Acq_Plan
65             (Provide_Acquisition_Data | Do_Not_Provide_Acquisition_Data)
66             | (Do_Not_Develop_Acq_Plan Do_Not_Provide_Acquisition_Data)
67             ),
68             (Execute_AoA
69             (Provide_AoA_Report | Do_Not_provide_AoA_Report )
70             | (Do_Not_Execute_AoA Do_Not_Provide_AoA_Report)
71             )
72             }
73 ;
74
75 /*Data that they must have to complete their actions. */
76 COORDINATE $a: Provide_CONOPS FROM MTAB,
77             $b: Develop_Acq_Plan FROM PM
78             DO ADD $a PRECEDES $b;
79             OD;
80
81 COORDINATE $a: Do_Not_Provide_CONOPS FROM MTAB,
82             $b: Do_Not_Develop_Acq_Plan FROM PM
83             DO ADD $a PRECEDES $b;
84             OD;
85
86 COORDINATE $a: Provide_CONOPS FROM MTAB,
87             $b: Execute_AoA FROM PM
88             DO ADD $a PRECEDES $b;
89             OD;
90
91 COORDINATE $a: Do_Not_Provide_CONOPS FROM MTAB,
92             $b: Do_Not_Execute_AoA FROM PM
93             DO ADD $a PRECEDES $b;
94             OD;
95

```

Figure 65. Lines 62–95: ROOT Project Management

```

96 /*Office of Naval Research. Provides development and research data.
97 They can either provide the requested data or not provide the data.*/
98 ROOT ONR: (Research_Related_Work
99            (Provide_Related_Work_Data | Do_Not_Provide_Related_Work_Data)
100            | (Do_Not_Research_Related_Work Do_Not_Provide_Related_Work_Data)
101            )
102 ;
103
104 /*Data that they must have to complete their actions. */
105 COORDINATE $a: Provide_CONOPS FROM MTAB,
106             $b: Research_Related_Work FROM ONR
107             DO ADD $a PRECEDES $b;
108             OD;
109
110 COORDINATE $a: Do_Not_Provide_CONOPS FROM MTAB,
111             $b: Do_Not_Research_Related_Work FROM ONR
112             DO ADD $a PRECEDES $b;
113             OD;
114

```

Figure 66. Lines 96–114: ROOT Office of Naval Research

```

115 /*Requirements writer. Assigned by OPNAV. In charge of creating CDD.
116 They can either complete the CDD sections or not complete them.*/
117 ROOT ReqWriter: Establish_RWG
118     Start_CDD
119     {(Write_Operational_Context Complete_CDD
120      | Do_Not_Write_OC Do_Not_Complete_CDD
121      ),
122      (Write_Threat_Summary Complete_CDD
123      | Do_Not_Write_TS Do_Not_Complete_CDD
124      ),
125      (Write_Capability_Discussion Complete_CDD
126      | Do_Not_Write_CD Do_Not_Complete_CDD
127      ),
128      (Write_Program_Summary Complete_CDD
129      | Do_Not_Write_PS Do_Not_Complete_CDD
130      ),
131      (Write_Performance_Attributes Complete_CDD
132      | Do_Not_Write_PA Do_Not_Complete_CDD
133      ),
134      (Write_Other_System_Attributes Complete_CDD
135      | Do_Not_Write_OSA Do_Not_Complete_CDD
136      ),
137      (Write_Joint_Interoperability Complete_CDD
138      | Do_Not_Write_JI Do_Not_Complete_CDD
139      ),
140      (Write_Spectrum_Electromagnetic_Environmental Complete_CDD
141      | Do_Not_Write_SEE Do_Not_Complete_CDD
142      ),
143      (Write_Intelligence Complete_CDD
144      | Do_Not_Write_I Do_Not_Complete_CDD
145      ),
146      (Write_Weapon_Safety Complete_CDD
147      | Do_Not_Write_WS Do_Not_Complete_CDD
148      ),
149      (Write_Technology_Readiness Complete_CDD
150      | Do_Not_Write_TR Do_Not_Complete_CDD
151      ),
152      (Write_DOTmLPPF Complete_CDD
153      | Do_Not_Write_D Do_Not_Complete_CDD
154      ),
155      (Write_Program_Affordability Complete_CDD
156      | Do_Not_Write_PAF Do_Not_Complete_CDD
157      )
158     }
159 ;
160

```

Figure 67. Lines 115–160 ROOT Requirements Writer

```

161 /*Data that they must have to complete their actions. */
162 COORDINATE $a: Provide_CONOPS FROM MTAB,
163 $b1: Write_Operational_Context FROM ReqWriter,
164 $b2: Write_Performance_Attributes FROM ReqWriter,
165 $b3: Write_Other_System_Attributes FROM ReqWriter,
166 $b4: Write_Spectrum_Electromagnetic_Environmental FROM ReqWriter,
167 $b5: Write_Intelligence FROM ReqWriter,
168 $b6: Write_Weapon_Safety FROM ReqWriter,
169 $b7: Write_DOTmLPF FROM ReqWriter
170 DO ADD $a PRECEDES $b1,
171 $a PRECEDES $b2,
172 $a PRECEDES $b3,
173 $a PRECEDES $b4,
174 $a PRECEDES $b5,
175 $a PRECEDES $b6,
176 $a PRECEDES $b7;
177 OD;
178
179 COORDINATE $a: Provide_Threat_Data FROM Threat_SME,
180 $b: Write_Threat_Summary FROM ReqWriter
181 DO ADD $a PRECEDES $b;
182 OD;
183
184 COORDINATE $a1: Provide_Related_Work_Data FROM MTAB,
185 $a2: Provide_Related_Work_Data FROM ONR,
186 $b1: Write_Capability_Discussion FROM ReqWriter,
187 $b2: Write_Performance_Attributes FROM ReqWriter,
188 $b3: Write_Other_System_Attributes FROM ReqWriter,
189 $b4: Write_Joint_Interoperability FROM ReqWriter
190 DO ADD $a1 PRECEDES $b1,
191 $a2 PRECEDES $b1,
192 $a1 PRECEDES $b2,
193 $a1 PRECEDES $b3,
194 $a1 PRECEDES $b4;
195 OD;
196
197 COORDINATE $a: Provide_Acquisition_Data FROM PM,
198 $b1: Write_Program_Summary FROM ReqWriter,
199 $b2: Write_Program_Affordability FROM ReqWriter
200 DO ADD $a PRECEDES $b1,
201 $a PRECEDES $b2;
202 OD;
203
204 COORDINATE $a: Write_Capability_Discussion FROM ReqWriter,
205 $b: Write_Joint_Interoperability FROM ReqWriter
206 DO ADD $a PRECEDES $b;
207 OD;
208
209 COORDINATE $a: Provide_AoA_Report FROM PM,
210 $b: Write_Technology_Readiness FROM ReqWriter
211 DO ADD $a PRECEDES $b;
212 OD;

```

Figure 68. Lines 161–212: COORDINATE Requirements Writer

```

213
214
215 /*MARK traces that have all sections completed to complete the CDD.*/
216
217 IF #Complete_CDD >= 13 THEN MARK;
218
219 FI;
220
221
222

```

Figure 69. Lines 213–222: Mark Traces That Have All Sections Completed to Complete the CDD.

```

223 /*Map out risk of the CDD not being completed.
224 Used code from reference (3). Updated for data in this program.
225
226 /* Event attributes include likelihood and impact to calculate a
227 trace_risk_score, risk, and other attributes used in global
228 risk report. Attribute sum_risk_score stores the sum of the
229 trace risk scores. */
230
231 ATTRIBUTES {   number   likelihood, impact, trace_risk_score,
232                sum_risk_score, max_risk_score,
233                max_risk_trace_unique_number;
234            };
235
236 /*Values based on estimates from one CDD in process.
237 If the information was provided was complete and on time it was a risk likelihood of 0.1.
238 If it was on time but not complete it was a risk likelihood of 0.5.
239 If it was complete but not on time it was a risk likelihood of 0.3. */
240
241 COORDINATE $Provide_CONOPS: Analyze_Threats
242 DO $Provide_CONOPS.likelihood:= 0.1;
243   $Provide_CONOPS.impact:= 10;
244 OD;
245
246 COORDINATE $Provide_CONOPS: Provide_Related_Work_Data
247 DO $Provide_CONOPS.likelihood:= 0.1;
248   $Provide_CONOPS.impact:= 5;
249 OD;
250
251 COORDINATE $Provide_Fielding_Data: Provide_Acquisition_Data
252 DO $Provide_Fielding_Data.likelihood:= 0.5;
253   $Provide_Fielding_Data.impact:= 10;
254 OD;
255
256 COORDINATE $Provide_CONOPS:Write_Operational_Context
257 DO $Provide_CONOPS.likelihood:= 0.5;
258   $Provide_CONOPS.impact:= 10;
259 OD;
260
261 COORDINATE $Provide_CONOPS: Write_Performance_Attributes
262 DO $Provide_CONOPS.likelihood:= 0.5;
263   $Provide_CONOPS.impact:= 10;
264 OD;
265
266 COORDINATE $Provide_CONOPS: Write_Other_System_Attributes
267 DO $Provide_CONOPS.likelihood:= 0.5;
268   $Provide_CONOPS.impact:= 10;
269 OD;
270
271 COORDINATE $Provide_CONOPS: Write_Spectrum_Electromagnetic_Environmental
272 DO $Provide_CONOPS.likelihood:= 0.1;
273   $Provide_CONOPS.impact:= 3;
274 OD;
275

```

Figure 70. Lines 223–275: Risk of CDD Not Completed (1)

```

276 COORDINATE $Provide_CONOPS: Write_Intelligence
277 DO $Provide_CONOPS.likelihood:= 1.0;
278 $Provide_CONOPS.impact:= 5;
279 OD;
280
281 COORDINATE $Provide_CONOPS: Write_Weapon_Safety
282 DO $Provide_CONOPS.likelihood:= 1.0;
283 $Provide_CONOPS.impact:= 3;
284 OD;
285
286 COORDINATE $Provide_CONOPS: Write_DOTmLPF
287 DO $Provide_CONOPS.likelihood:= 1.0;
288 $Provide_CONOPS.impact:= 5;
289 OD;
290
291 COORDINATE $Provide_Threat_Data: Write_Threat_Summary
292 DO $Provide_Threat_Data.likelihood:= 1.0;
293 $Provide_Threat_Data.impact:= 10;
294 OD;
295
296 COORDINATE $Provide_Related_Work_Data: Write_Capability_Discussion
297 DO $Provide_Related_Work_Data.likelihood:= 0.7;
298 $Provide_Related_Work_Data.impact:= 10;
299 OD;
300
301 COORDINATE $Provide_Related_Work_Data: Write_Performance_Attributes
302 DO $Provide_Related_Work_Data.likelihood:= 0.7;
303 $Provide_Related_Work_Data.impact:= 7;
304 OD;
305
306 COORDINATE $Provide_Related_Work_Data: Write_Other_System_Attributes
307 DO $Provide_Related_Work_Data.likelihood:= 0.7;
308 $Provide_Related_Work_Data.impact:= 7;
309 OD;
310
311 COORDINATE $Provide_Related_Work_Data: Write_Joint_Interoperability
312 DO $Provide_Related_Work_Data.likelihood:= 0.7;
313 $Provide_Related_Work_Data.impact:= 10;
314 OD;
315
316 COORDINATE $Provide_Acquisition_Data: Write_Program_Summary
317 DO $Provide_Acquisition_Data.likelihood:= 0.5;
318 $Provide_Acquisition_Data.impact:= 10;
319 OD;
320
321 COORDINATE $Provide_Acquisition_Data: Write_Program_Affordability
322 DO $Provide_Acquisition_Data.likelihood:= 0.5;
323 $Provide_Acquisition_Data.impact:= 10;
324 OD;
325

```

Figure 71. Lines 276–325: Risk of CDD Not Completed (2)

```

326 COORDINATE $Provide_AoA_Report: Write_Technology_Readiness
327 DO $Provide_AoA_Report.likelihood:= 0.5;
328 $Provide_AoA_Report.impact:= 10;
329 OD;
330

```

Figure 72. Lines 326–330: Risk of CDD Not Completed (3)

```

331 /* Trace Risk Table and Summary */
332
333 TABLE event_risks { TITLE ("Event Risks");
334                     TABS string Event,
335                          string Likelihood,
336                          string Impact,
337                          string Risk_Score;
338                     };
339
340 CLEAR event_risks;
341
342 COORDINATE $e: $$EVENT
343
344 DO trace_risk_score+= ($e.likelihood*$e.impact);
345 IF ($e.likelihood*$e.impact) > 0 THEN
346     event_risks <|
347         Event: SAY($e),
348         Likelihood: SAY($e.likelihood),
349         Impact: SAY($e.impact),
350         Risk_Score: SAY($e.likelihood*$e.impact);
351 FI;
352
353 /* If the TRACE RISK SCORE for a given trace exceeds the
354 current global maximum risk factor value (initialized
355 at zero), then make the max risk factor THIS trace's
356 risk factor and get its trace id for the max risk trace. */
357 IF trace_risk_score > GLOBAL.max_risk_score THEN
358     GLOBAL.max_risk_score:= trace_risk_score;
359     GLOBAL.max_risk_trace_unique_number:= trace_id;
360 FI;
361
362 /*MARK traces that have a risk factor greater than a certain value*/
363
364 /*IF trace_risk_score >= 9 THEN MARK; FI;*/
365
366 OD;
367
368 /* If there is a risk to the trace then show the risk table on the
369 trace and say the totl trace risk. */
370 IF trace_risk_score > 0 THEN SHOW event_risks;
371 SAY("Total Trace Risk: "trace_risk_score);
372 FI;
373

```

Figure 73. Lines 331–373: Risk Table and Summary

```

380 /* Create and display Global Risk Report */
381
382 GLOBAL
383
384 REPORT Global_Risk { TITLE ( "Risk Report for Scope " $$scope ); };
385
386 /* Include these SAY statements in the Global Risk Report */
387 SAY("Total risk over " #$$TRACE " traces (sum of trace risk scores): "
388     GLOBAL.sum_risk_score
389     => Global_Risk;
390 SAY("Highest Risk: " GLOBAL.max_risk_score (trace "
391     GLOBAL.max_risk_trace_unique_number")")
392     => Global_Risk;
393 SAY("Average Risk: " GLOBAL.sum_risk_score/#$$TRACE)
394     => Global_Risk;
395 SAY("Sort by Marked to view traces with above average risk >=9.")
396     => Global_Risk;
397
398 SHOW Global_Risk;
399

```

Figure 74. Lines 380–399: Calculate Total Risk

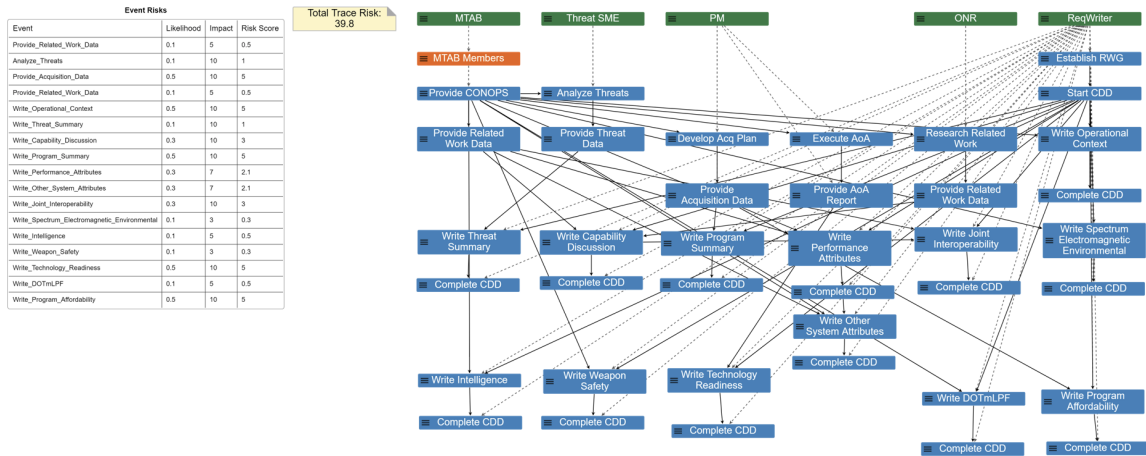


Figure 75. Trace 1: CDD Completed

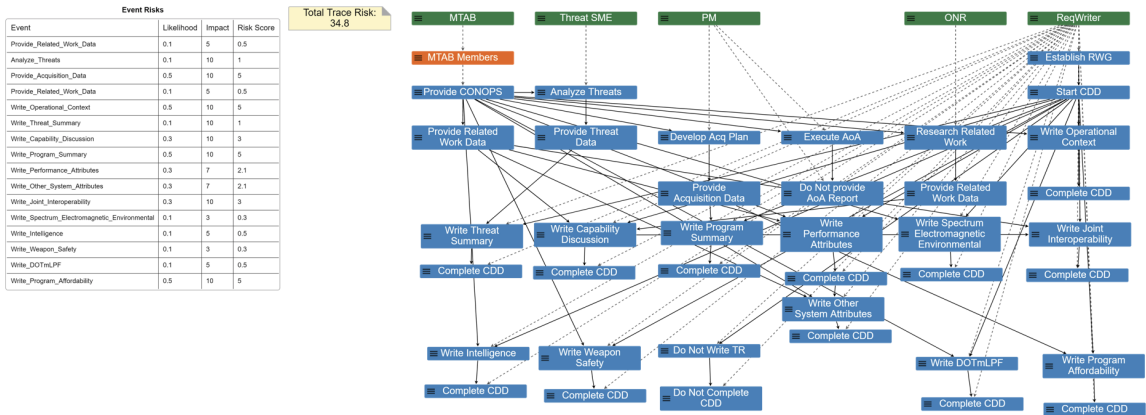


Figure 76. Trace 2: AoA Not Provided. CDD Not Completed.

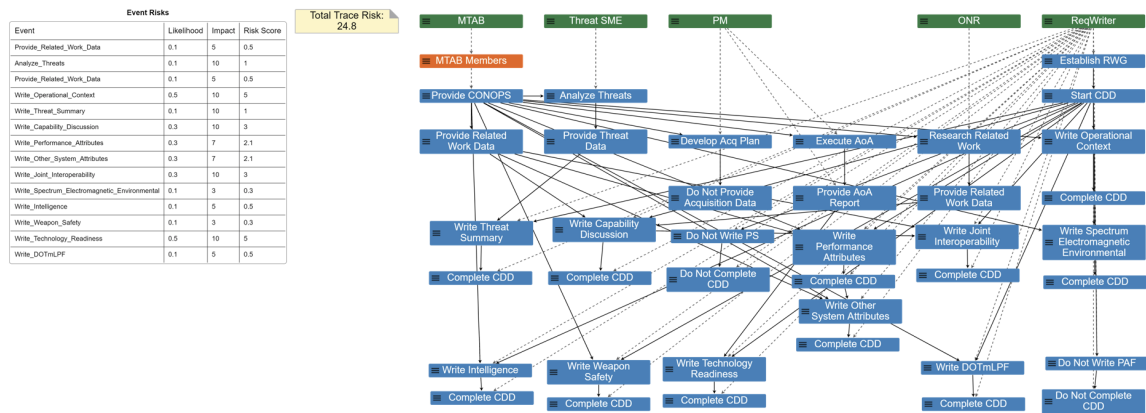


Figure 77. Trace 3: Acquisition Plan Not Provided. CDD Not Completed.

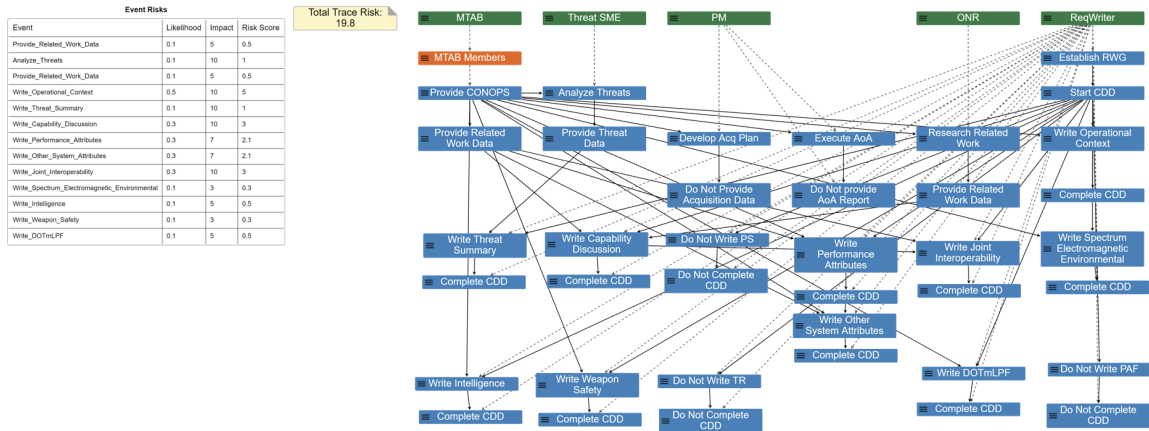


Figure 78. Trace 4: Acquisition Plan and AoA Not Provided. CDD Not Completed.

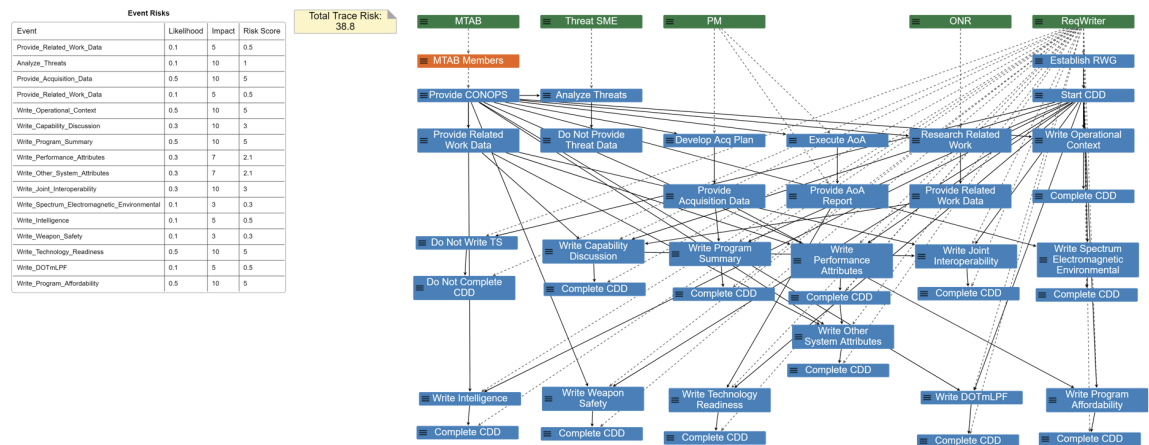


Figure 79. Trace 5: Threat Summary Not Provided. CDD Not Completed.

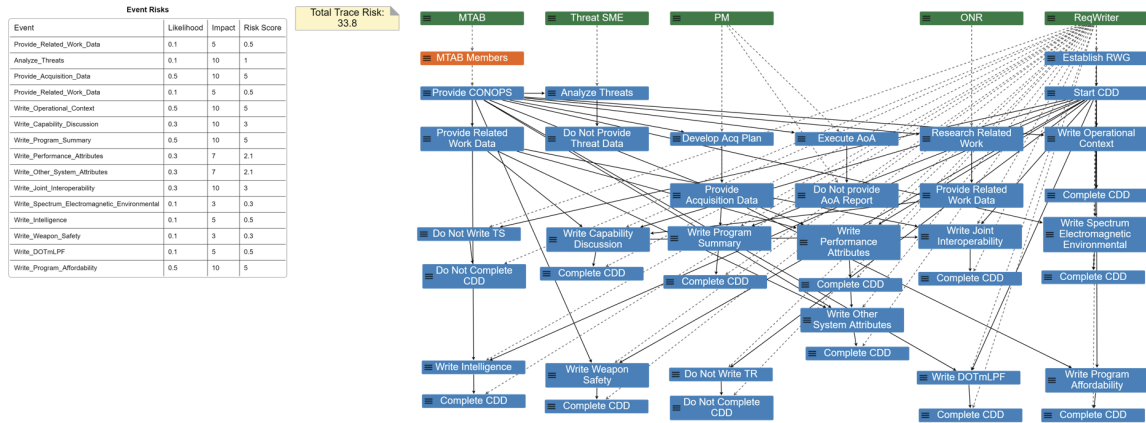


Figure 80. Trace 6: Threat Summary and AoA Not Provided. CDD Not Completed.

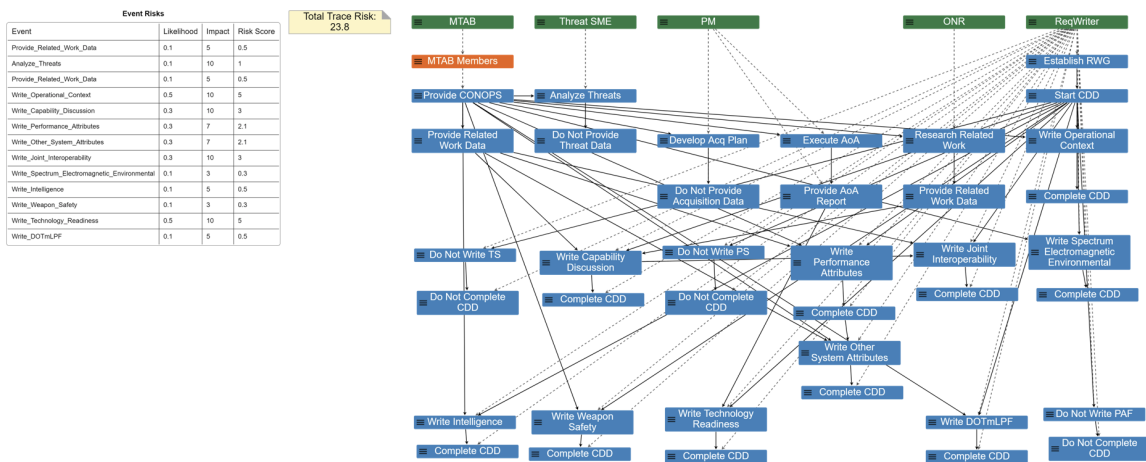


Figure 81. Trace 7: Threat Summary and Acquisition Plan Not Provided. CDD Not Completed.

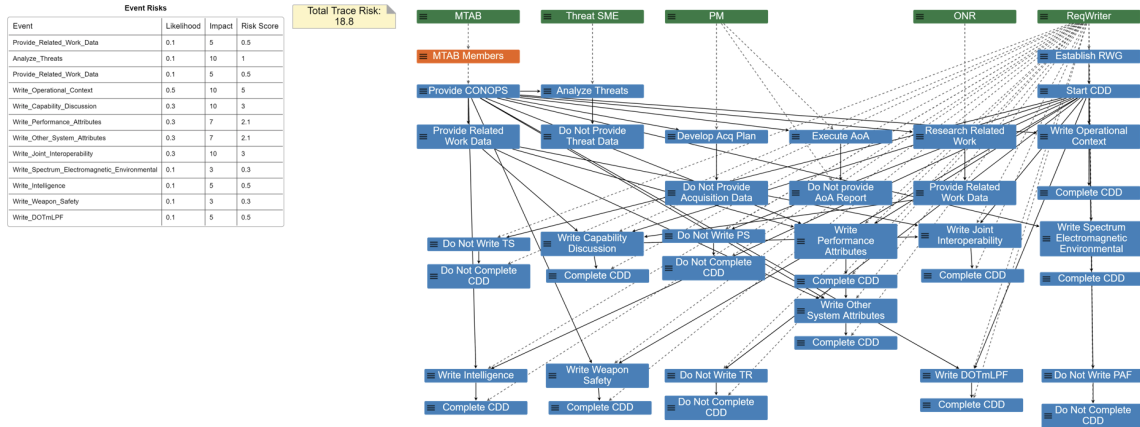


Figure 82. Trace 8: Threat Summary, Acquisition Plan, and AoA Not Provided. CDD Not Completed.

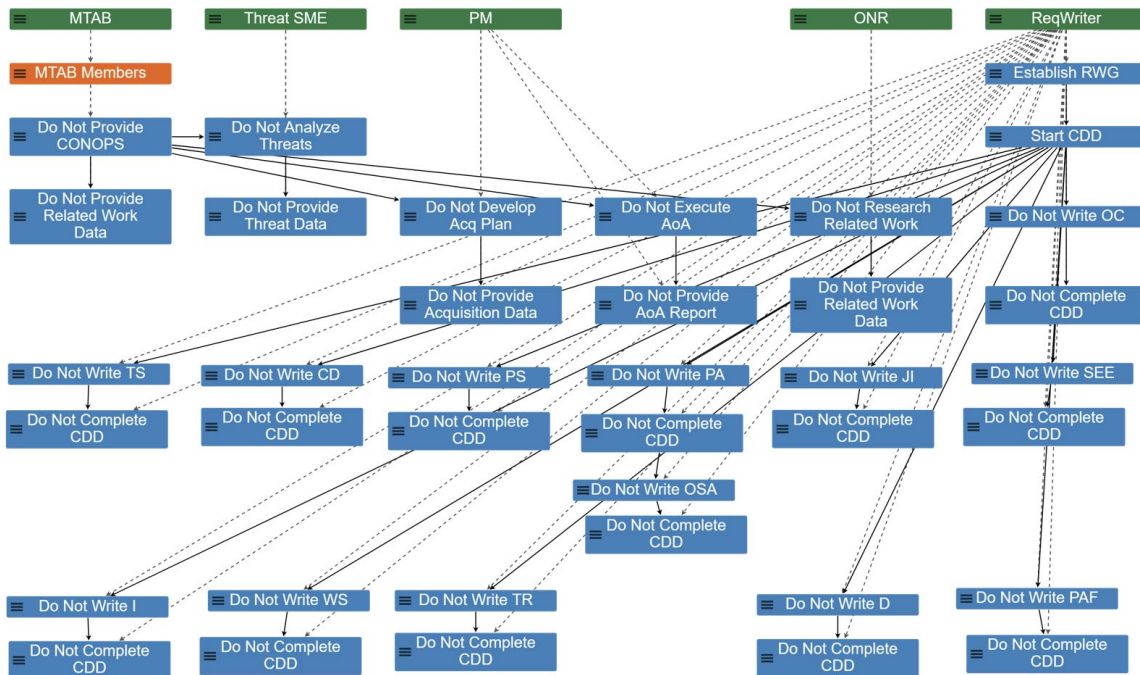


Figure 83. Trace 9: CONOPS Not Provided. CDD Not Completed.

```

1  /* Hazard Rapid Large Area Clearance Locate *****Latest Version 20211129 0030
2
3  SE3650 Team 5 project
4
5  Team Members: Angel Gill, Alexander Fedorovich, Andrew Machamer,
6  Geoffrey Eberle, Mary Mesa
7
8  Test the behavior for locating hazards in a search area. This simplified model
9  is used to determine a robust system for locating hazards.
10
11 Run at Scope 1: Local scope is used to scan additional grids with each
12 type. The time constraint is set to 20 minutes.
13
14 Emergent behavior:
15 (1) UGV is not always chosen as there is not a coordinate statement
16 mandating its use. This mirrors what is seen in real life where
17 tendency is to revert to handheld unless told to do otherwise.
18 Making a constraint mandating its use would be required for
19 this to occur.
20 (2) Worst case scenario is scope 1 trace 42 when no equipment
21 is deployed. Due to bad conditions, sensitive hazards, UGV
22 not deployed.
23 (3) Running at multiple scopes does not change traces as number of
24 scans is set to go no higher than 2. Traces above 20 minutes
25 are also not allowed.
26 (4) UAV is fastest equipment. It can detect max hazards in 10 minutes.
27 Hand held equipment takes 20 minutes.
28 (5) It is not possible for UGV to find max hazards. It takes too long.
29
30 Results:
31
32 Maximum number of grids possible to be scanned is 6. Maximum number of
33 hazards that can be located is 5. The highest success rate is 5 grids
34 scanned and 5 hazards located.
35
36 References:
37 Example 24: ATM Withdrawal Component Diagram
38
39 */

```

Figure 84. RLAC MP Code Lines 1–39

```

40
41 SCHEMA Rapid_Large_Area_Clearance_of_Hazards_Locate
42
43 /*Define environmental conditions.*****
44 ROOT Environment: Weather_Conditions;
45                   Weather_Conditions:
46                     ( Good_Conditions | Bad_Conditions )
47 ;
48
49 /*Define hazard conditions. *****
50 ROOT Hazard: Hazard_Type;
51              Hazard_Type:
52                ( Sensitive | Nonsensitive )
53 ;
54
55 /*Define attributes to be tracked. *****
56 ATTRIBUTES { interval time, max_grids_scanned, max_hazards_located,
57              max_time, min_time; }
58 ;
59
60 /*Define time parameters for using hand held equipment. *****
61 Handheld_Report_hazard_location: BUILD{ time: = 10;};
62
63 Handheld_No_hazard_located: BUILD{ time: = 5;};
64
65 /*Setup case for using hand held equipment. This also defines probability
66 of detection at 95% and sets the local scope two.*****
67 ROOT Handheld_Equipment: (Handheld_Proceed_to_search_area |
68                           Handheld_No_Deploy);
69
70                           Handheld_Proceed_to_search_area:
71                           (* < 2 > Handheld_Scan_grid
72                             ( <<0.95>> Handheld_Detect_hazards
73                               Handheld_Report_hazard_location|
74                               <<0.05>> Handheld_No_hazards
75                               Handheld_No_hazard_located
76                             )
77                           *)
78
79 /* Create local report for time required to scan grids and how many hazards
80 were located in the grids. Design constraint. */
81 BUILD {
82   COORDINATE $hazards: ( Handheld_Report_hazard_location|
83                         Handheld_No_hazard_located)
84   DO time += $hazards.time;
85   SAY($hazards " occurred with time " time " minutes");
86 OD;
87 SAY ("Handheld Number of Grids Scanned: " #Handheld_Scan_grid);
88 SAY ("Handheld Number of Hazards located: " #Handheld_Detect_hazards);
89 ENSURE time > 0 AND time <= 20;
90 }
91 ;

```

Figure 85. RLAC MP Code Lines 40–91

```

92 /* Define constraint that Handheld will not deploy when sensitive hazards
93 are present. Simplification constraint. */
94 COORDINATE $a: Sensitive FROM Hazard,
95 $b: Handheld_No_Deploy FROM Handheld_Equipment
96 DO ADD $a PRECEDES $b; OD;
97
98 /*Define time parameters for using UAV equipment. *****/
99 UAV_Report_hazard_location: BUILD{ time: = 5;};
100 UAV_No_hazard_located: BUILD{ time: = 5;};
101
102 /*Setup case for using UAV. *****/
103 ROOT UAV_Equipment: (UAV_Proceed_to_search_area |
104 UAV_No_Deploy );
105
106 UAV_Proceed_to_search_area:
107 (* < 2 > UAV_Scan_grid
108 ( <<0.6>> UAV_Detect_hazards
109 UAV_Report_hazard_location|
110 <<0.4>> UAV_No_hazards
111 UAV_No_hazard_located )
112 *)
113
114 /* Create local report for time required to scan grids and how many hazards
115 were located in the grids. Design constraint.*/
116 BUILD{
117 COORDINATE $hazards: ( UAV_Report_hazard_location|
118 UAV_No_hazard_located )
119 DO time += $hazards.time;
120 SAY($hazards " occured with time " time " minutes");
121 OD;
122 SAY ("UAV Number of Grids Scanned: " #UAV_Scan_grid);
123 SAY ("UAV Number of Hazards located: " #UAV_Detect_hazards);
124 ENSURE time > 0 AND time <= 20;
125 }
126 ;
127
128 /* Define constraint that UAV will not deploy when bad weather
129 conditions exist. Simplification constraint. */
130 COORDINATE $a: Bad_Conditions FROM Environment,
131 $b: UAV_No_Deploy FROM UAV_Equipment
132 DO ADD $a PRECEDES $b; OD;
133
134 /*Define time parameters for using UGV equipment. *****/
135 UGV_Report_hazard_location: BUILD{ time: = 15;};
136 UGV_No_hazard_located: BUILD{ time: = 10;};
137

```

Figure 86. RLAC MP Code Lines 92–137

```

138 /*Setup case for using UGV.*****/
139 ROOT UGV_Equipment:      (UGV_Proceed_to_search_area |
140                           UGV_No_Deploy);
141
142       UGV_Proceed_to_search_area:
143       (* < 1..2 > UGV_Scan_grid
144         ( <<0.8>> UGV_Detect_hazards
145           UGV_Report_hazard_location |
146           <<0.2>> UGV_No_hazards
147           UGV_No_hazard_located      )
148         *)
149
150 /* Create local report for time required to scan grids and how many hazards
151 were located in the grids. Design constraint.*/
152 BUILD{
153     COORDINATE $hazards: ( UGV_Report_hazard_location|
154                           UGV_No_hazard_located)
155     DO time += $hazards.time;
156     SAY($hazards " occured with time " time " minutes");
157     OD;
158     SAY ("UGV Number of Grids Scanned: " #UGV_Scan_grid);
159     SAY ("UGV Number of Hazards located: " #UGV_Detect_hazards);
160     ENSURE time > 0 AND time <= 20;
161 }
162 ;
163

```

Figure 87. RLAC MP Code Lines 138–163

```

164 /*Calculate and mark items of interest on traces.*****/
165 max_grids_scanned += #Handheld_Scan_grid +
166                     #UAV_Scan_grid + #UGV_Scan_grid;
167 max_hazards_located += #Handheld_Detect_hazards +
168                       #UAV_Detect_hazards + #UGV_Detect_hazards;
169
170 SAY ("Total Number of Grids Scanned: " max_grids_scanned);
171 SAY ("Total Number of Hazards located: " max_hazards_located);
172
173 COORDINATE $e: $$EVENT
174
175     DO max_time := ($e.time);
176
177     IF max_grids_scanned >= GLOBAL.max_grids_scanned THEN
178         GLOBAL.max_grids_scanned := max_grids_scanned;
179
180     IF max_hazards_located > GLOBAL.max_hazards_located THEN
181         GLOBAL.max_hazards_located := max_hazards_located;
182
183     FI;
184
185     FI;
186
187     IF max_time > GLOBAL.max_time THEN
188         GLOBAL.max_time := max_time;
189     FI;
190 OD;
191
192 IF max_grids_scanned > 4 AND
193 max_hazards_located > 3
194     THEN MARK;
195 FI;
196

```

Figure 88. RLAC MP Code Lines 164–196

```

197 /* Setup Composite Diagram *****/
198
199 GRAPH Diagram { TITLE ("Key Player Interactions");};
200
201     COORDINATE $E1: ($$ROOT | $$COMPOSITE) DO
202     COORDINATE $E2: ($$ROOT | $$COMPOSITE) DO
203     WITHIN Diagram
204     {
205     /* For each valid event trace find all root and composite
206     event instances within the event trace and add them to the graph. */
207         Node$a: LAST ($E1);
208         Node$b: LAST ($E2);
209     /* LAST option in the node constructors ensures there will be only
210     a single instance of a node in the graph for each root and composite
211     event found in the event trace */
212
213     /* If event E1 is IN another event E2, add an arrow "E2 calls E1" */
214     IF $E1 IN $E2 THEN
215         ADD Node$b ARROW("calls") Node$a;
216     FI;
217
218     /* Look for interactions between components and data structures.
219
220     Interactions between components, usually are represented by coordination of
221     events in the interacting components (presence of PRECEDES between events
222     in different threads).
223
224     Interactions between components and data structures are modeled by shared events,
225     since data structures are usually modeled as a set of operations performed on them. */
226
227         IF $E1 != $E2 AND
228         NOT ($E1 IN $E2 OR $E2 IN $E1) AND
229         ( ( EXISTS $E3: $$EVENT ($E3 IN $E1 AND $E3 IN $E2) ) OR
230         ( EXISTS $E3: $$EVENT FROM $E1,
231           $E4: $$EVENT FROM $E2 ($E3 PRECEDES $E4) ) ) THEN
232         ADD Node$a LINE("interacts with") Node$b;
233     FI;
234
235     }; /* end WITHIN Diagram */
236 OD; /* end of $E1 and $E2 loops */
237
238

```

Figure 89. RLAC MP Code Lines 197–238

```

239 /*Setup Global Report. *****/
240 GLOBAL
241
242 REPORT Statistics { TITLE ("Maximum Search Area");};
243
244 SAY ("Maximum grids scanned " GLOBAL.max_grids_scanned) => Statistics;
245 SAY ("Maximum hazards located " GLOBAL.max_hazards_located) => Statistics;
246 SAY ("In " GLOBAL.max_time " minutes.") => Statistics;
247 SAY( "Total Traces " #$$TRACE) => Statistics;
248
249 SHOW Statistics;
250
251 SHOW Diagram;
252
253 SHOW ACTIVITY DIAGRAM Handheld_Equipment, UAV_Equipment, UGV_Equipment, Environment,
254 Hazard;

```

Figure 90. RLAC MP Code Lines 239–254

LIST OF REFERENCES

- AFCEC. 2018. *Functional Requirements Documents Standard Operating Procedure 10–601*. Washington, DC: Air Force Civil Engineer Center.
- Agile Business Consortium. 2022. “Requirements and User Stories.” Accessed April 8, 2022. https://www.agilebusiness.org/page/ProjectFramework_15_RequirementsandUserStories
- Alden, Nathaniel and Rachel Talkington. 2020. “Model of Supply Chain with Two Cyber Threats.” Monterey Phoenix. Created 5 July 2020. <https://staging.firebird.nps.edu/project/fca31185-207c-48c1-bd49-1bc86ece35e9>
- Army. 2018. *Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology) Middle-Tier Acquisition Policy*. Washington, DC: Office of the Assistant Secretary of the Army. <https://aida.mitre.org/wp-content/uploads/2018/10/MTA-ASAALT-Policy-25-Sep-18-3.pdf>
- ASN. 2018. *Middle Tier Acquisition and Acquisition Agility Guidance*. Washington, DC: The Assistant Secretary of the Navy. https://www.dau.edu/tools/Documents/Interactive%20Adaptive%20Acquisition%20Framework%20Chart/Resources/Navy_Middle_Tier_Guidance.pdf
- Auguston, Mikhail. “ATM Withdrawal with Global Graph.” Accessed April 4, 2022. <https://staging.firebird.nps.edu/project/0f7d58d5-8fbd-4ee8-82b3-a4bf877f9765>
- Blanchard, Benjamin S. and Wolter J. Fabrycky. 2011. *Systems Engineering and Analysis*. Upper Saddle River, New Jersey: Prentice Hall.
- Brackens, Brian. 2022. “Air Force to Deliver Vehicle That Uses Laser to Clear Bombs.” Air Force Life Cycle Management Center Public Affairs. <https://www.wpafb.af.mil/News/Article-Display/Article/2925421/air-force-to-deliver-vehicle-that-uses-laser-to-clear-bombs/>
- Brooks F.P., Jr., 1986. “No Silver Bullet: Essence and Accidents of Software Engineering.” Accessed Aug 4, 2022. <http://www.cs.unc.edu/techreports/86-020.pdf>
- Buede, Dennis M., and William D. Miller. 2016. *The Engineering Design of Systems: Models and Methods*. 3rd ed. Hoboken, NJ: Wiley.
- Chief Information Officer. 2010. *DOD Architecture Framework Version 2.02*. Last modified August 2010. <https://dodcio.defense.gov/Library/DOD-Architecture-Framework>

- CJCS. 2016. *Doctrine for Joint Explosive Ordnance Disposal*. JP 3-42. Washington, DC: Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_42.pdf
- Cliff, Roger, Mark Burles, Michael S. Chase, Derek Eaton, Kevin L. Pollpeter. 2007. *Entering the Dragon's Lair. Chinese Anti-Access Strategies and Their Implications for the United States*. RAND Corporation. <https://www.rand.org/pubs/monographs/MG524.html>
- Crawley, Edward, Bruce Cameron, Daniel Selva. 2016. *System Architecture Strategy and Product Development for Complex Systems*. Hoboken, NJ: Pearson.
- DAG. 2021. *Defense Acquisition Guidebook*. Accessed 5 Sep 2021. <https://www.dau.edu/tools/dag>
- DAU. 2014. "Systems Engineering Process." Accessed on April 1, 2022. <https://www.dau.edu/acquipedia/pages/ArticleContent.aspx?itemid=204>
- Department of Defense. 2021. *DOD Executive Agent for the Military Explosive Ordnance Disposal Technology and Training*. DOD Directive 5160.62. Washington, DC: Office of the Under Secretary of Defense Policy. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/516062Ep.PDF?ver=STxBEKUXrBCBhS6C8jEw%3D%3D>
- Edson, Robert and Frittmann, Jaime. 2010. "Illustrating the Concept of Operations (CONOPs) Continuum and Its Relationship to the Acquisition Life-cycle." Proceedings from the Seventh Annual Acquisition Research Symposium, Monterey, CA. <http://hdl.handle.net/10945/33465>.
- Goddin, John. 2017. "Remote Mass Mechanical Clearance Makes Clearing UXO From Airfields Safer and Faster." Air Force Civil Engineer Center. <https://www.afcec.af.mil/News/Video/video/563494/>
- Hart, Laura E. 2015. "Introduction To Model-Based System Engineering (MBSE) and SysML." Presented at the Delaware Valley INCOSE Chapter Meeting. July 30, 2015. <https://www.incose.org/docs/default-source/delaware-valley/mbse-overview-incose-30-july-2015.pdf>
- Hitchins, Derek. 2007. *Systems Engineering A 21st Century Systems Methodology*. West Sussex, England: John Wiley and Sons, Ltd.
- . 2019. "Rigorous Soft Methodology." Systems World. Accessed May 8, 2022. <https://systems.hitchins.net/systems/systems-methodology/rigorous-soft-methodology.html>
- Hoff, Patrick R. 2009. "Translation of User Needs to Systems Requirements." Master's thesis, Naval Postgraduate School. <https://calhoun.nps.edu/handle/10945/4928>

- INCOSE. 2012. *Guide to Writing Requirements*. Requirements Working Group International Council on Systems Engineering (INCOSE).
<https://www.incose.org/docs/default-source/ProductsPublications/systems-engineering-measurement-primer---december-2010.pdf>
- ISO/IEC/IEEE 29148:2011E. 2018. *International Standard - Systems and Software Engineering -- Life Cycle Processes -- Requirements Engineering*. IEEE.
<https://doi.org/10.1109/IEEESTD.2018.8559686>.
- Innoslate. 2021. “Why Innoslate.” Accessed 11 Jul 2022. <https://www.innoslate.com/why-innoslate/>
- Intellipedia. 2021. *Manual for the Operation of the Joint Capabilities Integration and Development System*. https://intellipedia.intelink.gov/wiki/Joint_Capabilities_Integration_and_Development_System
- JBER Public Affairs. 2019. “PACAF Cultivates CE Airmen With Ground-Breaking RADAS Training.” Joint Base Elmendorf-Richardson Public Affairs.
<https://www.af.mil/News/Article-Display/Article/1744946/pacaf-cultivates-ce-airmen-with-ground-breaking-radas-training/>
- JEOD. 2005. *JEOD Initial Capabilities Document*. Ser No. 671–75-05. JROCM 151–05. Knowledge Management and Decision Support (KMDS).
- JEOD. 2017. *Department of Defense Explosive Ordnance Disposal Program Board Policy Agreement 5100.01*. Department of Defense Explosive Ordnance Disposal Program Board.
- Kitowska, Klaudia. 2022. “How to Write (Actually) Useful Software Requirements Specification” *BOOST HIGH* (blog), Accessed 8 April 2022.
<https://boosthigh.com/software-requirements-specification/>
- Lundquist, Ned. 2021. “Subsea Defense: Navy Deepens Commitment to Underwater Vehicles.” Marine Link. February 15, 2021. <https://www.marinelink.com/news/subsea-defense-navy-deepens-commitment-485303>
- Malatesta, CAPT Dan. 2021. “PMS 408 Expeditionary Missions.” Presentation at Sea Air Space, National Harbor, MD, April 2021. Accessed on May 28, 2022.
<https://www.navsea.navy.mil/Portals/103/Documents/Exhibits/SAS2021/SAS2021-Expeditionary%20Missions.pdf>
- MARCORSYSCOM. 2020. *MARCORSYSCOM Acquisition Guidebook*. Marine Corps Systems Command. <https://www.marcorsyscom.marines.mil/Portals/105/HOMEMCSC/FY21-01%20MAG%20v1.0%2020201030.pdf?ver=qXiYXXTwtK32bWq6loT5IQ%3D%3D>

- Mooz, Hal and Kevin Forsberg. 2006. *The Dual Vee - Illuminating the Management of Complexity*. Sixteenth Annual International Symposium of the International Council on Systems Engineering (INCOSE), 8–14.
- Naval Postgraduate School. 2022. “Monterey Phoenix Home.” Accessed 11 July 2022. <https://wiki.nps.edu/display/MP/Monterey+Phoenix+Home>
- NAVSEA. 2021. “Warfare Centers NSWC Indian Head: History of EOD.” Accessed Jan 17, 2021. <https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Indian-Head/What-We-Do/Technical-Departments/EOD-Dept/Joint-Service-EOD-Technology-Program/>
- NAVSEA. 2022. “Who We Are. Headquarters.” Accessed March 2022. <https://www.navsea.navy.mil/who-we-are/headquarters/>
- Nguyen, Hoa G. et al. 2019. “A Compact End Cryptographic Unit for Tactical Unmanned Systems. *Unmanned Systems Technology XXI*, July 11, 2019, Proc. SPIE 11021. <https://www.ll.mit.edu/r-d/publications/compact-end-cryptographic-unit-tactical-unmanned-systems>
- NSWC IHD Public Affairs. 2021. “NSWC IHD’s EOD Department Hosts EOD Threat Expo.” Naval Sea Systems Command. <https://www.navsea.navy.mil/Media/News/SavedNewsModule/Article/2577426/nswc-ihs-eod-department-hosts-eod-threat-expo/>
- ONR. 2022. “Explosive Hazards Defeat.” Accessed 1 April 2022. <https://www.onr.navy.mil/Science-Technology/Departments/Code-32/all-programs/explosive-hazard-defeat-systems>
- OPNAV. 2021. *Top-Level Requirements Development and Approval*. Chief of Naval Operations. <https://www.secnav.navy.mil/doni/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-400%20Organization%20and%20Functional%20Support%20Services/5420.119.pdf>
- Reese, Cody M. 2018. “Development of System-Level Requirements and Effectiveness Measures for an Amphibious Fuel Distribution System.” Master’s thesis, Naval Postgraduate School. <https://calhoun.nps.edu/handle/10945/60452>
- SEBoK. 2021. “Guide to the Systems Engineering Body of Knowledge (SEBoK).” Last modified May 19, 2021, [https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_\(SEBoK\)](https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)).
- Sharma, Richa. 2017. *Grounding Functional Requirements Classification in Organizational Semiotics*. In *Interdisciplinary Approaches to Semiotics*, edited by Asun Lopez-Varela Azcarate, London, England: IntechOpen, 2017. 10.5772/67608. <https://www.intechopen.com/chapters/54479>

- Shell. 2021. Enclosure F - Department of Defense Explosive Ordnance Disposal Technology Requirements Development. OPNAV N957.
- Stevens, Roger. T. 1979. *Operational Test and Evaluation: A Systems Engineering Process*. New York, NY: Wiley.
- Swan, Jonathan M. 2017. "Analysis of the Requirements Generation Process for the Logistics Analysis and Wargame Support Tool." Master's thesis, Naval Postgraduate School https://calhoun.nps.edu/bitstream/handle/10945/55542/17Jun_Swan_Jonathan.pdf?sequence=1&isAllowed=y
- Ulrich, Karl T., and Steven D. Eppinger. 2016. *Product Design and Development*. New York, NY: McGraw-Hill Education.
- USAASC. 2022. "Man Transportable Robotic System Increment II (MTRS Inc II)." Accessed May 2022. <https://asc.army.mil/web/portfolio-item/man-transportable-robotic-system-increment-ii/>
- USMC. 2017. "Combat Development Command Bulletin 5400. Requirements Transition Process." Commanding General, Marine Corps Combat Development Command. Last modified May 31, 2017. <https://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/FDSP/FDS%20References/CDCBul%205400.pdf?ver=2018-05-01-115226-690>
- Walden, David D., Roedler, Garry J., Forsberg, Kevin J, Hamelin, R. Douglas, and Shortell, Thomas M. 2015. *Systems Engineering Handbook A Guide for System Life Cycle Processes and Activities*. Hoboken, NJ: John Wiley and Sons, Inc.
- Weck, Oliver L. de. "Fundamentals of Systems Engineering. Session 1" *Massachusetts Institute of Technology*. Fall 2015. https://ocw.mit.edu/courses/16-842-fundamentals-of-systems-engineering-fall-2015/resources/mit16_842f15_ses1se_ovr_vw/
- Weisman, Lynsi. 2017. "Statement of Work Explosive Ordnance Disposal Threat Exposition and Policy Agreement Objectives." NSWC Indian Head EOD Technology Division Contract No. N0017417C0014.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

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