NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A PROBABILITY RISK ASSESSMENT TO SUPPORT A DEFENDABLE AND QUANTITATIVE SAFETY ASSESSMENT OF THE ASSAULT AMPHIBIOUS VEHICLE

by

Joseph A. Dean

September 2018

Thesis Advisor: Bryan M. O'Halloran
Co-Advisor: Douglas Van Bossuyt

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
A PROBABILITY RISK ASSESSMENT TO SUPPORT A DEFENDABLE AND QUANTITATIVE SAFETY ASSESSMENT OF THE ASSAULT AMPHIBIOUS VEHICLE

5. FUNDING NUMBERS

6. AUTHOR(S) Joseph A. Dean

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)

There is a significant delta between the acknowledged probability of potential mishaps under the current safety assessment approach derived from Military Standard (MIL-STD) 882E, *Department of Defense Standard Practice of System Safety*, and what is observed from actualized mishaps reported for the assault amphibious vehicle (AAV). All of the previously investigated AAV mishaps were the result of a chain of events that could not be traced back to a single initiating mechanism, which is the approach MIL-STD-882E uses. This thesis sets out to determine the core elements of a risk-based safety assessment method that is most suitable for the AAV. By decomposing actual mishap reports, we identified common failure modes that were not adequately assessed under the current process. We then applied a probabilistic risk assessment approach and a supporting human reliability assessment to the mishap reports. This method, and the subsequent probabilistic risk assessment of these mishaps, suggests a greater probability of the unwanted event of an AAV sinking than previously acknowledged. The framework outlined in this paper has the ability to provide a more accurate and quantifiable risk assessment.

14. SUBJECT TERMS mishaps, MIL-STD-882E, system safety, failure modes, probabilistic risk assessment, human reliability assessment	**15. NUMBER OF PAGES** 95
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A PROBABILITY RISK ASSESSMENT TO SUPPORT A DEFENDABLE AND QUANTITATIVE SAFETY ASSESSMENT OF THE ASSAULT AMPHIBIOUS VEHICLE

Joseph A. Dean
Civilian, Department of the Navy
BLibStud, University of Mary Washington, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2018

Approved by: Bryan M. O'Halloran
Advisor

Douglas Van Bossuyt
Co-Advisor

Ronald E. Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

There is a significant delta between the acknowledged probability of potential mishaps under the current safety assessment approach derived from Military Standard (MIL-STD) 882E, *Department of Defense Standard Practice of System Safety*, and what is observed from actualized mishaps reported for the assault amphibious vehicle (AAV). All of the previously investigated AAV mishaps were the result of a chain of events that could not be traced back to a single initiating mechanism, which is the approach MIL-STD-882E uses. This thesis sets out to determine the core elements of a risk-based safety assessment method that is most suitable for the AAV. By decomposing actual mishap reports, we identified common failure modes that were not adequately assessed under the current process. We then applied a probabilistic risk assessment approach and a supporting human reliability assessment to the mishap reports. This method, and the subsequent probabilistic risk assessment of these mishaps, suggests a greater probability of the unwanted event of an AAV sinking than previously acknowledged. The framework outlined in this paper has the ability to provide a more accurate and quantifiable risk assessment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....2
B. RESEARCH QUESTION....2
C. SUMMARY OF CONTRIBUTIONS....2

II. LITERATURE REVIEW....5
A. DEFINING TERMS....5
B. REVIEW OF EXISTING RISK AND SAFETY METHODOLOGIES....6
1. Subsystem Hazard Analysis (MIL-STD-882E)....7
2. System Hazard Analysis (MIL-STD-882E)....7
3. Operating and Support Hazard Analysis (MIL-STD-882E)....8
4. Failure Mode and Effects Analysis / Failure Mode Effects, and Criticality Analysis....8
5. Fault Tree Analysis....8
6. Event Tree Analysis....9
7. Probabilistic Risk Assessment....9
C. DESIRED ATTRIBUTES....10
D. RELATED RESEARCH....11
E. SUMMARY OF METHODOLOGIES....12

III. RESEARCH DESIGN....13
A. AAV OPERATIONS....13
B. MISHAPS....14
1. Mishap #1....14
2. Mishap #2....15
3. Mishap #3....16
4. Mishap #4....16
C. MISHAP DECOMPOSITION....16
D. SUMMARY....19

IV. METHODOLOGY....21
A. FRAMEWORK....21
1. Step 1: Data Collection....23
2. Step 2: Mishap Scenario Models....23
3. Step 3: Identify Failure Modes....25

4. Step 4.a: Calculate Hardware and Software Probability of Failure Distribution....30
5. Step 4.b: Collect or Conduct Human Task Analyst....30
6. Step 5: Conduct PRA....32
7. Step 6: Programmatic Decision on Risk Acceptance....34
B. SUMMARY....34

V. DISCUSSION....37

VI. CONCLUSION....39

APPENDIX A. MISHAP #1....41
A. MISHAP #1 DECOMPOSITION....41
B. MISHAP #1 MISHAP SCENARIO MODEL....44
C. MISHAP #1 FAILURE MODES....45

APPENDIX B. MISHAP #2 DECOMPOSITION....47

APPENDIX C. MISHAP #3....51
A. MISHAP #3 DECOMPOSITION....51
B. MISHAP #3 MISHAP SCENARIO MODEL....53
C. MISHAP #3 FAILURE MODES....54

APPENDIX D. MISHAP #4....57
A. MISHAP #4 DECOMPOSITION....57
B. MISHAP #4 MISHAP SCENARIO MODEL....61
C. MISHAP #4 FAILURE MODES....62

APPENDIX E. MISHAP #2 CUT SET—SAPHIRE DATA....65

LIST OF REFERENCES....73

INITIAL DISTRIBUTION LIST....75

LIST OF FIGURES

Figure 1. Mishap Assessment Method 22

Figure 2. Mishap #2 Scenario 24

Figure 3. Maintenance—Plenum Bolts Not Installed FTA 26

Figure 4. Pre-water Ops Check FTA 26

Figure 5. Vehicle Batteries Discharge FTA 27

Figure 6. Loss of Bilge Capacity FTA 28

Figure 7. Mishap #2 Event Tree 29

Figure 8. Mishap #2 Scenario 44

Figure 9. Operation—Water Rushes in through Open Hatch 45

Figure 10. Mishap #1 Event Tree 46

Figure 11. Mishap #3 Scenario 53

Figure 12. Maintenance—Hydraulic Leak 54

Figure 13. Pre-water Ops—Plenum 54

Figure 14. Mishap #3 Event Tree 55

Figure 15. Mishap #4 Scenario 61

Figure 16. Operation—Water Rushes in through Open Hatch 62

Figure 17. Mishap #4 Event Tree 63

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Desired Methodology Characteristics.....10

Table 2. NARA Generic Task List. Source: Kirwan et al. (2005).....31

Table 3. Mishap #2 Cut Set.....33

Table 4. Mishap Probability Summary 35

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAV	assault amphibious vehicle
CC	crew chief
CREAM	Cognitive Reliability and Error Analysis Method
DoD	Department of Defense
DoN	Department of the Navy
ETA	event tree analysis
FMEA	failure mode effects and analysis
FMECA	failure mode, effects and criticality analysis
FTA	fault tree analysis
HRA	human reliability analysis
HTS	hazard tracking system
LSD	Dock Landing Ship
MIL-STD	military standard
NARA	Nuclear Action Reliability Assessment
O&SHA	operating and support hazard analysis
PRA	probabilistic risk assessment
SHA	system hazard analysis
SOP	standard operating procedure
SPAR-H	Standard Plant Analysis Risk HRA Method
SSHA	subsystem hazard analysis
THERP	Technique for Human Error Rate Prediction
VC	vehicle commander
VEH	vehicle

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The risks associated with the equipment provided to the warfighter is often articulated and acknowledged differently from the risks realized during its operation. Military Standard (MIL-STD) 882E, the *Department of Defense Standard Practice of System Safety*, is the standard methodology utilized for assessing the safety of the systems that are provided to the warfighter. MIL-STD-882E (Department of Defense 2012) details the process for the identification, assessment, and mitigation of risks associated with the development, test, production, use, and disposal of the system. The MIL-STD is a simplistic approach that focuses on single-point system failures. Its application during the design phase works well in identifying catastrophic single-point failures that are often designed out or substantially mitigated to reduce the probability of occurrence. The direct causative relationship between a mishap and the single-point failure mechanism generally guides systems engineers to design a system that has a very low probability of occurrence of single-point failures.

The research presented here analyzes real-world assault amphibious vehicle (AAV) mishaps to identify conditions, factors, root causes, and trends that lead to mishaps, which then informs the development of a risk-based method that is better suited to identify potential mishaps and determine the probability of occurrence for the mishaps with respect to the AAV. The goal of the research presented in this thesis is to develop a risk-informed safety method that more accurately captures the comprehensive risk to AAV crews during operation of the system.

This thesis focuses on four reported mishaps resulting in AAV sinkings. Each mishap is decomposed to the basic chain of events that led to the sinking. Several conditions that are common across the four mishaps are identified. These conditions generally shared the same casual factors including:

- poor quality control during maintenance operations
- failure to conduct pre-operations check/pre-water operations check

Both of the above listed conditions share a common human related cause – a human error or human violation of established policy and procedures. Human error can be further characterized as either skill-based, judgement, or misperception. Assault amphibious vehicle operations rely heavily on policy and procedures to mitigate known hazards, but existing AAV safety analysis does not acknowledge human error, policy, or protocol violation as a mishap triggering mechanism. Additionally, each of the identified hazards is treated as independent events while most mishap reports indicate a common cause relationship between multiple human-initiated mishaps. Existing MIL-STD-882E safety analysis of the AAV does not recognize the relationship or dependency between one human error or violation occurring and subsequent human errors or violations leading to a mishap.

This thesis proposes a method for legacy system managers to close the gap between the risks that are formally identified through methods such as MIL-STD-882E and mishaps that occur during system operation. Mishap scenario models built by dissecting the system mishap reports are a core component of the proposed method presented herein. However, it is the belief of the author that the method may be applicable anywhere in the system design process as long as there is sufficient data to construct applicable mishap scenario models. For example, operational concepts, architectural views, and historical data on similar in-service systems may be utilized to develop preliminary mishap scenario models for a system that is in development. The fidelity of preliminary mishap scenario models is expected to increase as the system architecture is defined and the system baseline is developed, thus allowing the method to be applied through the design phase in an effort to refine the resulting risk analysis.

The results from the proposed method on the AAV mishaps provide a quantitative assessment of the chain of events that are specific to the operation of the as-produced and as-operated AAV that were not previously captured or acknowledged in official safety analysis of the AAV. Table 1 presents the probability of each investigated mishap with respect to the outcome of an unwanted sinking event of an AAV. Please note that while the analysis presented in this thesis is realistic, no conclusions should be drawn from the analysis for the purposes of AAV operations.

Table 1. Mishap Probability Summary

Mishap	Probability	MIL-STD-882E Probability Category
#1	9.15E-02	B
#2	2.6472E-06	D
#3	2.09952E-06	D
#4	3.02E-04	D

By assuming the calculated probabilities shown in Table 1 are within the acceptable order of magnitude and the severity of the mishap is catastrophic based on the credible consequence of loss of life for mishaps related to sinking of a vehicle, the mishap risks identified in Table 1 are categorized as 1B, 1D, 1D, and 1D, respectively, per MIL-STD-882E. These risks can then in turn be put in the weighted organizational matrix based on value of the capability provided by the system as currently designed, the probability and severity of a mishap occurring, and the cost of fixing or mitigating the risk.

The decomposition of realized mishaps and the subsequent probabilistic risk assessment and human reliability analysis of the analyzed mishaps suggest a greater probability of the unwanted event of an AAV sinking than previously acknowledged. Additionally, if the newly identified risks are deemed unacceptable, this quantitative assessment has identified high-risk events on which AAV program managers and systems engineers can focus resources in support of improving safety.

Reference

Department of Defense. 2012. *System Safety*. DoD MIL-STD-882E. Washington, DC: Department of Defense.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The risks formally associated with the equipment provided to the warfighter are often articulated and acknowledged differently from the risks realized during its operation. Military Standard (MIL-STD) 882E, *Department of Defense Standard Practice of System Safety* (Department of Defense [DoD] 2012), is the standard methodology utilized for assessing the safety of the systems that are provided to the warfighter. MIL-STD-882E details the process for the identification, assessment, and mitigation of risks associated with the development, test, production, use, and disposal of a system. MIL-STD-882E focuses on single-failure events but does not generally include failure modes that require sequential failure events to occur. The application of MIL-STD-882E during the design phase of the systems engineering process works well for identifying catastrophic single-point failures that are then often designed out or substantially mitigated to reduce the probability of occurrence. The direct causative relationship between a mishap and the single-point failure mechanism generally guides systems engineers to design a system that has a very low probability of occurrence of single-point failures. In this situation, the calculated probability of a mishap occurring using the MIL-STD-882E is much lower than what is observed in the field.

For example, consider the assault amphibious vehicle (AAV). Despite several AAVs having sunk in the past, all identified risks relating to the sinking of the AAV are currently assessed as medium (1E) risks in accordance with MIL-STD-882E (AAV, unpublished data, March 18, 2016). Medium 1E risk means catastrophic severity with a probability of improbable. However, based on AAV mishaps that have occurred, there is an argument to reassess the probability of occurrence of mishaps. The discrepancy between the risk identified in MIL-STD-882E and the observed risk is a result of MIL-STD-882E not taking into account failure modes that require sequential failure events to occur. The AAV mishaps reviewed as part of this thesis are all the result of a chain of events that cannot not be traced back to a single-point failure.

The purpose of this research is to analyze real-world AAV mishaps to identify conditions, factors, root causes, and trends that lead to the mishaps, which then informs the

development of a risk-based method that is better suited for assessing risk for the AAV. Once a core understanding of why the mishaps occur and why they are not well represented in existing MIL-STD-882E safety analyses, this research analyzes existing risk assessment methods for their applicability in identifying and quantifying mishaps that otherwise would be missed in formal safety analysis. The decomposition of the AAV mishaps included in this thesis does not to divulge specific information on individual incidents, but rather is used to identify generalized trends and causes that are useful to this research.

A. PROBLEM STATEMENT

There is a significant difference between the acknowledged probability of potential mishaps under the current safety assessment approach and what is observed from actualized mishaps reported. MIL-STD-882E focuses on single-point failures but does not generally include failure modes that require sequential failure events to occur. The application of MIL-STD-882E during the design phase of the systems engineering process works well in identifying catastrophic single-point failures that are then often designed out or substantially mitigated to reduce the probability of occurrence. The direct causative relationship between a mishap and the single-point failure mechanism generally guides systems engineers to design a system that has a very low probability of occurrence of single-point failures. However, the culmination of several failures as reported in mishap reports are often ignored.

B. RESEARCH QUESTION

What are the core elements of a risk-based safety assessment method that are most suitable for an AAV?

C. SUMMARY OF CONTRIBUTIONS

The "DoD requires program offices to support system related mishap investigations by providing analyses of the hazards that contributed to the mishap" (DoD 2012, 14). However, a much greater understanding of the system and its failure modes can be obtained by analyzing the mishap report directly. The mishap reports provide a level of detail

regarding the relationship between the operator, the system, and the operating environment that the systems engineer may not be aware of or understand. There is an opportunity to establish a method for breaking down such mishap reports to identify relevant system information to quantify the probability of mishaps that have already been observed to occur again in the future. Through a methodical analysis of mishap reports, program managers and users will be better informed of the current risks of their systems as designed and operated. Additionally, it may be possible to identify high-risk events in advance thus allowing engineers to focus resources in support of improving safety.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

The literature review in this section provides relevant background on current risk assessment methodologies to identify what are the core elements of a risk-based method that are most suitable for an AAV. The objective is to identify core elements of risk-based methods and apply a method for breaking down mishap reports to quantify the probability of the actualized mishaps. This thesis proposes a method for legacy system managers to close the gap between the risks that are formally identified through methods such as MIL-STD-882E and mishaps that occur during system operation. Through a methodical analysis of mishap reports, program managers and users will be better informed of the current risks of their systems as designed and operated. Additionally, it may be possible to identify high-risk events in advance thus allowing engineers to focus resources in support of improving safety.

A. DEFINING TERMS

MIL-STD-882E (DoD 2012) defines the terms below as follows:

- Mishap: "A mishap is the event resulting in unintentional death, injury, damage to or loss of equipment or property, or damage to the environment" (6).
- Hazard: "A hazard is the condition that leads to the event" (5).
- Causal factor. "A causal factor is the mechanism that triggers the hazard" (4).

MIL-STD-882E presents a singular linear relationship between the mechanism that triggers a hazard and the resulting mishap. However, in all of the mishap reports reviewed as part of this research, there are no single-point failures. In all cases, multiple failures occurred to cause the mishap. In practice, it appears that mishaps are much more dynamic; two or more failure events contribute to a mishap occurring. In an effort to move beyond the single-point failure analysis language found in MIL-STD-882E, the author proposes using the following definitions which will be used for the remainder of this thesis:

- Mishap: A mishap is defined as the sequence of hazards that must occur for a system to be in a failed state. In the context of this research, a failed state is defined as the system of interest being sunk or damaged beyond immediate repair and/or the loss of life.

- Hazard: The hazard is defined as the failure event or events that contributed to the mishap.

- Causal factor: The causal factor is the initiating event that triggers the hazard(s) that leads to the mishap occurring.

B. REVIEW OF EXISTING RISK AND SAFETY METHODOLOGIES

The methodology that the DoD uses is MIL-STD-882E which is structured specifically for assessing "the severity category and probability level of the potential mishap(s) for each hazard across all of the system modes" (DoD 2012, 10) using the severity and probability definitions found in the standard. From analysis of the available AAV mishap reports (see Chapter III for a detailed analysis of mishap reports), it can be surmised that the mishaps are not the result of a single realized hazard, but rather from a series of hazards initiated by a causal factor. The series of hazards and causal factor generally are a combination of hardware failures and human failures. Additionally, in most cases the hardware failure may also be linked to a human failure.

Ideally a risk assessment should include a technique to model the entire operational phase of a system that accounts for hazards and causal factors including both human failure events hardware failure events, and can examine mishaps that require sequential failure events and causal factors to be present in order for the mishap to occur. This section reviews several pertinent existing methodologies and their applicability to mishaps that are caused by sequential failure events and causal factors. The following paragraphs include an analysis of key attributes and deficiencies of existing methodologies.

1. Subsystem Hazard Analysis (MIL-STD-882E)

The subsystem hazard analysis (SSHA) in MIL-STD-882E is a potential technique for capturing some of the human reliability issues. The purpose of the SSHA, per MIL-STD-882E, is to "identify hazards associated with the design of the subsystem, and the human is considered a component within a subsystem, receiving both inputs and outputs" (DoD 2012, 51). A main objective of this analysis is to "determine modes of failure, including component failure modes and human errors, single-point and common mode failures, the effects when failures occur in subsystem components, and from functional relationships between components and equipment comprising each subsystem" (DoD 2012, 51). However, MIL-STD-882E does not call out a specific type of analysis to accomplish this task; the standard only states that the results shall "be captured in the hazard tracking system (HTS)" (52). The HTS only presents a singular linear relationship between the causal factors, hazards, and mishaps, per MIL-STD-882E. As a result, a mishap that consists of sequential failure events and causal factors cannot be accounted for using SSHA.

2. System Hazard Analysis (MIL-STD-882E)

The system hazard analysis (SHA) is also described in MIL-STD-882E where it is stated that the SHA shall "identify hazards and mitigation measures in the integrated system design, including software and subsystem and human interfaces" (DoD 2012, 54). Additionally, MIL-STD-882E states that the SHA shall identify "possible independent, dependent, and simultaneous events, including system failures, failures of safety devices, common cause failures, and system interactions that could create a hazard or result in an increase in risk" (54). However, the standard does not specify an analysis method to accomplish this task; it only states that the results shall "be captured in the HTS" (55). The structure of the HTS does not allow for the identification of dependent causal factors leading to a potential mishap, thus making SHA not particularly useful for situations where sequential failure events and causal factors must occur to result in a specific mishap.

3. Operating and Support Hazard Analysis (MIL-STD-882E)

The operating and support hazard analysis (O&SHA) found in MIL-STD-882E is intended to "identify and assess hazards introduced by operational and support activities" (DoD 2012, 57). Similar to the SSHA, the O&SHA states that "the human shall be considered an element of the total system" (DoD 2012, 57). However, the O&SHA also inherits all the other deficiencies that are found and are discussed above the SSHA and SHA. MIL-STD-882E does not specify a technique to accomplish O&SHA, and results are reported in the HTS in the same way that results are presented in SSHA and SHA.

4. Failure Mode and Effects Analysis / Failure Mode Effects, and Criticality Analysis

The failure mode effects and analysis (FMEA) and the failure mode, effects and criticality analysis (FMECA) are bottom up evaluation techniques that focus on the design and function of a system (Ericson 2005). "The purpose of FMEA/FMECA is to evaluate the effect of failure modes to determine if a design change is necessary due to unacceptable reliability, safety, or operation" (Ericson 2005, 236). FMEA/FMECA is generally performed by listing out the components of the system, then identifying failure modes, failure rates, immediate effects, and system effects for each component. However, FMEA/FMECA is poor at identifying failure modes that require multiple components to fail or failure modes that include both hardware component failures and human failures (Ericson 2005). While FMEA/FMECA excels at considering single-point failures, FMEA/FMECA is not a satisfactory tool for analyzing failure modes that are caused by multiple failure events.

5. Fault Tree Analysis

Fault tree analysis (FTA) is a top-down method for identifying causative paths from a failure event to all possible root causes (Ericson 2005). FTA is useful in that if done correctly, FTA can model a combination of casual factors or basic events that can cause a failure event to occur and provide a quantifiable probability of occurrence of the failure event. However, there is a limitation in theory since the goal of the FTA is to identify the

probability of occurrence of a specified failure event. Subsequent failure events not identified or associated with the specified failure event may be neglected.

6. Event Tree Analysis

Event tree analysis (ETA) is used to identify and evaluate all possible paths from an initiating event to either an acceptable system state or a failed system state. Many different outcome paths from a single initiating event can be identified and the probability of occurrence can be determined for each outcome. ETA can be limited if an analyst needs to evaluate the consequences of multiple initiating events, as a single ETA is limited to one initiating event or one group of similar initiating events. However, this limitation is mitigated by conducting multiple ETAs and combining their results as necessary.

7. Probabilistic Risk Assessment

As described in the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, probabilistic risk assessment (PRA) is a "comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance" (Stamatelatos 2011, 1-1). PRA is a logic-based modeling approach constructed using sets of scenarios, frequencies of occurrence, and consequences. PRA is an extension of the FTA and ETA methods discussed above. A PRA identifies an initiating event and one or more top-level events that lead to a predicted end state using the ETA methodology. The initiating event requires some type of required response from the system, subsystem, or operator. The response is the top-level event. The top-level event has a success or failure probability based on its response to the initiating event or preceding event. This allows for the calculation of probability of success or failure at the top-level events and through to the various end states. The PRA is not limited in the number of initiating events or any dependency among initiating events. The top-level events generally connect to FTAs where basic events are mapped to calculate probabilities of specific sequences of basic events occurring which results in the failure of the top-level event in the event tree. The PRA has the ability to support a comprehensive view of the various end states as derived from the various sequence of basic events.

It is difficult to fully assess the safety of a system's design without considering the reliability of the human within the system. The PRA forces the analyst to incorporate human involvement at the relevant top-level events that require a response from the operator. Quantifying the reliability of the human within the system is a potential challenge. However, human reliability analysis (HRA) is often incorporated within a PRA to address such issues (Stamatelatos 2011). There are numerous HRA modeling approaches such as, THERP, HEART, HEARTH, SPAR-H and CREAM, each with its own technique or guidance for quantifying human error probability for specific human actions or events. HRA models often focus on a specific type of human systems integration and associated task descriptions. Assessing and identifying suitable HRA models that support PRA adds another layer of complexity in conducting a complete and valid PRA.

C. DESIRED ATTRIBUTES

The ideal safety assessment method for the AAV shall be a comprehensive analysis method focused on identifying and assessing the probability of a mishap that has either occurred or could be predicted to occur. The method shall be able to model the hardware, software, and human dependencies within the entire system. Single failure events and sequential failure events shall be identified, assessed, and recorded. The goal of the method is to support a risk-informed safety case that more accurately captures the sequential and parallel failure event pathways that are observed in the operation of the system. Table 1 illustrates the correlation between the desired characteristics and the methodologies.

Table 1. Desired Methodology Characteristics

Methodology	Hardware, Software, and Human Dependencies	Single Failure Events	Sequential Failure Events	Comprehensive Parallel Event Probability
SSHA		X		
SHA		X		
O&SHA		X		
FMEA/FMECA		X		
FTA	X	X	X	
ETA	X	X	X	
PRA	X	X	X	X

D. RELATED RESEARCH

Industry has long embraced the benefit of performing a PRA in the development of certain products or procedures such as nuclear power plants, aircraft, spacecraft, and automobiles/passenger vehicles. There is an abundance of literature on PRA specific to various products and procedures from automobiles to medical procedures. Subsequently, research into human reliability analysis has also grown. Specific HRA techniques have been developed to further quantify and increase the accuracy of specific PRA models. For example, "Human Error Probability Estimation for Process Risk Assessment with Emphasis on Control Room Operations" (Nespoli and Sabatino 2010), "Application of the CARA HRA Tool to Air Traffic Management Safety Cases" (Gibson and Kirwan 2008), "Human Error Probability Assessment During Maintenance Activities of Marine Systems" (Islam et al. 2018) leveraged existing HRA techniques such as, Technique for Human Error Rate Prediction (THERP), Cognitive Reliability and Error Analysis Method (CREAM), Nuclear Action Reliability Assessment (NARA), and Standard Plant Analysis Risk HRA Method (SPAR-H) to model the human reliability within their systems.

Mishap analysis research is often centered on the human component of the system. For example, "Simulation and Analysis of Class A and B Flight Mishaps with an Assessment of Human Factors Intervention" (Jensen 1999) and "A Human Systems Integration Perspective to Evaluating Naval Aviation Mishaps and Developing Intervention Strategies" (Cowan 2009) both analyze mishap reports. However, their focus is the evaluation of the human casual factors and identification of related HRA techniques. Such research is beyond the scope of this paper as substantial resources and time would be required to specifically tailor an existing HRA technique to the AAV operations.

In summary, while many methods exist in the literature that may be useful in specific situations, a holistic method applicable to analyzing AAV mishaps does not currently exist. Of the methods that do exist, the primary focus on aspects of human reliability other than probability of mishaps. As a result, this research focuses on the quantification of mishap probability for AAV operations.

E. SUMMARY OF METHODOLOGIES

The current safety assessment state of practice for the AAV is largely influenced by MIL-STD-882E. There are analyses, such as the SHA and O&SHA, referenced within MIL-STD-882E that in theory could be executed in a comprehensive, structured, and logical method if preformed using the FTA or ETA methods, but the reporting structure of the HTS restricts the assessment to a single linear relation between a hazard and a mishap. The MIL-STD-882E structure for identifying and tracking risks within the HTS focuses on single hazards that lead to mishaps which negates the usefulness of more comprehensive, structured, and logical methods in association with HTS and MIL-STD-882E. To support the communication of the results of a more comprehensive analysis, the HTS will need to be restructured. FTA and ETA have their own deficiencies as previously identified that prevent them from being an all-inclusive method. PRA shows the most potential in correcting the deficiency between the acknowledged risk and the actual risk found in current safety analyses of the AAV. Thus, there is motivation to develop a PRA-based method specific to the operational scenarios of the AAV system and decomposed AAV mishap reports that may help program managers and system designers to better understand and improve the safety of the AAV, and further may provide a method that can be used during the design of a replacement for the AAV (or similar systems) to avoid some of the mishaps that have occurred with the AAV. A PRA-based method may provide program managers and other stakeholders with a method that better informs stakeholders of the current risks of systems as designed and operated. Additionally, high-risk events may be identifiable in advance of a mishap, thus allowing engineers to focus resources in support of improving system safety.

III. RESEARCH DESIGN

All of the AAV mishaps investigated as part of this research are found to be the result of a chain of events that cannot not be traced back to a single casual factor. The MIL-STD-882E safety methodology lacks the ability to identify, assess, and mitigate mishaps where more than one hazard or causal factor is needed to realize the mishap. The purpose of this research is to analyze real-world AAV mishaps to identify conditions, factors, root causes, and trends that lead to the mishaps in an attempt to identify a risk-based method that is better suited for the AAV.

A. AAV OPERATIONS

Am understanding of AAV operations is necessary to comprehend the sequence of events that comprise mishap reports. The AAV is an armored tracked amphibious assault landing vehicle that carries troops from ship to shore, through rough water and the surf zone, and inland to objectives after the AAV is ashore (USMC 2012). While performing water operations, the AAV is partially submerged with approximately 18 inches of the hull above the water line.

The AAV is normally embarked and transported on amphibious warfare ships. The most common type of AAV embarkation aboard amphibious ships is conducted by entering the water from land and transiting out through the surf zone where the vehicle is put into neutral to disable the tracks and water jets are engaged to propel the AAV forward to an offshore anchored ship (USMC 2013). The vehicle commander is required to complete a standard pre-operation checklist and will ensure the watertight integrity of the AAV before entering the water (DoN 2012b). A group of AAVs maintain a designated interval upon entering the water and travel in a column to facilitate ease of loading. The lead AAV positions off the ship's stern and awaits the signal to load. Upon notification that the ship is ready for embarkation, the AAVs proceed to the ship for loading. The driver places the vehicle in first gear to engage tracks before entering the ship and proceeds until tracks touch down within the well deck. Embarked personnel remain aboard the AAVs until all

the vehicles are embarked and stopped, and authorization to move about the well-deck has been given.

AAVs are launched from the ship and transition to their objective on land in a process called debarkation. In this process, the AAVs have already been embarked on to the ship and are staged in the well deck. The crew conducts the required pre-water operations checks and waits for permission to launch. Once permission is granted, the driver places the vehicle in water tracks mode and drives off out of the well deck of the ship into the water where it briefly submerges. The typically AAV surfaces uneventfully and is transitioned to the objective ashore (USMC 2012).

B. MISHAPS

The formal mishap investigative report provides a detailed fact-based chronological history of the vehicle and crew. The analysis of the reports allows the identification of the contributing conditions and associated causal factors.

The following are brief descriptions of several relevant mishaps. For practical purposes, these mishaps are referred to as mishap #1, #2, #3, and #4.

1. Mishap #1

This event occurred during the debarkation portion of an amphibious operation (Commanding General Second Marine Division 1994). The AAVs had already embarked to the ship and were staged in the well deck. The crew conducted the required pre-water operations checks and waited for permission to launch. Once permission was granted, the crew launched the vehicle from the well deck and it surfaces uneventfully. The driver placed vehicle gear selector in neutral position while accelerator pedal was completely depressed and pushed the hand throttle all the way forward and removed his foot from the accelerator pedal. The driver unlocked and opened his hatch. The driver turned his body in a clockwise direction until facing aft in an attempt to secure his hatch in the open position. At this time, the driver experienced difficulty in securing his hatch due to a missing driver's hatch support. Meanwhile, the vehicle commander (VC) and crew chief (CC) were facing aft locking their hatches simultaneously with the driver. The VC turned forward and

noticed water up to driver's hatch and warned the driver he is about to get wet. The driver turned forward just as water began rushing into driver's hatch. The driver turned towards the CC chief with a look of panic and confusion. The VC and CC attempted to take corrective action but were unsuccessful due to the volume of water rushing in through the driver's hatch. The vehicle submerged completely.

2. Mishap #2

This event occurred during the embarkation portion of an amphibious operation (Bourne 2009). In this mishap, the engine of the vehicle stalled as it approached the stern gate of the ship. Immediate attempts by the driver to restart the vehicle failed. The vehicle rotated and floated partially into the well deck. Over the next 5–10 minutes, the wave action in the well deck moved the vehicle about the well deck. The crew of vehicle reported that they felt jarring and impact with the ship. The starboard forward bilge outlet cover assembly was torn off of the vehicle unknown to the crew. The vehicle then floated out of the well deck. At this point the vehicle had no hydraulic bilge capability due to the stalled engine and limited electric bilge capacity, and had no communications due to a discharged battery bank. A second vehicle moved in to tow the vehicle. The first attempt to tow the vehicle into the well deck was turned away because of the depth of water at the sill of the ship was insufficient. The remaining AAVs continued to load while the ship ballasted down to increase the depth of the water at the sill. Approximately 35 minutes passed between the time the vehicle was rigged for tow and the final recovery attempt. Once the ship ballasted to the proper depth, the tow vehicle made its final approach with disabled vehicle in tow. The starboard bilge drain of the disabled vehicle submerged as a function of both the increased draft from the excess sea water taken on over the previous 35 minutes, and the increased pressure on the bow from both wind and seas. The first tow line broke as the tow vehicle made contact with the stern gate and the disabled vehicle was simultaneously hit with a large wave. The tow vehicle was then pulled backward and slightly down the stern gate causing the second towline break. The bow of disabled vehicle continued to rotate downward, and within 3–5 seconds the entire vehicle had submerged.

3. Mishap #3

This mishap occurred during a training evolution called basic water training (Strack 2010). Basic water training familiarizes future AAV crewmen with the water operations of the vehicle. Under the supervision of an instructor, students drive the AAV into the water and perform a series of maneuvers. In this situation, as the student driver drove the vehicle into the ocean nearing the end of the surf zone, the vehicle started to take on water at a rapid pace overwhelming the vehicle's bilge capacity. The vehicle took a nose down angle and sank at the edge of the surf zone approximately 2–3 minutes after entering the water.

4. Mishap #4

Similar to mishap #3, this mishap occurred during the basic water training evolution (Seiffert 2011). In this situation, the student driver drove into the water, and the vehicle started floating. The driver was instructed to put the gear selector in neutral and to open his hatch. The driver was then instructed to drive straight out and conduct a turn. After the turn, the instructor noticed the water rising over the bow of the vehicle and instructed the driver to let off the throttle. The driver reported that the throttle pedal was stuck and attempted to free the pedal. Meanwhile, the water rose further and started to flow into the driver's hatch. The driver became unresponsive to instructions. The instructor unsuccessfully attempted corrective action due to the flow of water into the driver's hatch. The vehicle submerged completely.

C. MISHAP DECOMPOSITION

Each of these mishaps is unique in their own way. None of them are as a result of single casual factors, but rather each mishap is the result of a series of casual factors unfolding over varying periods of time. When reviewing a mishap report, it is often challenging to distinguish when chains of events leading to mishaps were originally initiated. In an attempt to better understand the factors involved in each of these mishaps, a reverse engineering approach is utilized. Starting with the end result of the unwanted event and working backwards to identify the different potential factors is proposed as a method of better understanding the mishaps. The investigative reports developed in accordance with *Judge Advocate General Instruction 5800.7F* (DoN 2012a),

section 0209.d are the primary records utilized to decompose the events that led to the mishaps. The formal mishap investigative report provides a detailed fact-based chronological history of the vehicle and crew. The details in the mishap investigation report are communicated in two forms; *findings of facts* and *opinions*. The findings of facts are specific facts relevant to times, places, persons, and events leading up to and following the event under investigation. The findings of facts are generally related to prior maintenance activities (M), pre-operation checks (P), events (E), and recovery (R). The opinions (O) are reasonable evaluations, inferences, or conclusions of the investigating officer based on the facts found. An in-depth analysis of the formal mishap investigation report allows the analyst to identify key elements among the findings and opinions that contributed to the mishap.

The first step in the decomposition of the mishap is the extraction of the relevant findings. The relevant findings are limited to system related operations, procedures, functions, and conditions. In this context the system includes the vehicle and operator. Findings regarding the operator are focused on his or her actions or tasks as they relate to the operation of the system. All findings that identify a potential contributing conditions and subsequent causal factors to such are noted. These key elements can be organized to illustrate a logical flow of cause and effect throughout the buildup of the mishap.

The sequence of events articulated in the mishap investigation reports in comparison with standard operating procedures (SOPs) and pre-operation checklists are essential in creating a complete and inclusive mishap decomposition. Deviations from SOPs and pre-operation checklists are often captured as findings within mishap reports, but not always. A key feature of SOPs and pre-operation checklists is that if a component or task is highlighted within, it must be critical to the safe operation of the vehicle.

The second step involves assessing the investigating officer's opinions from the report and comparing them to the conditions and potential causal factors extrapolated from the findings. This comparison validates the identification of conditions and casual factors and can potentially reveal a previously dismissed factor. At this point the extraction and organization of the findings and opinions resemble a logical sequence of events. All conditions contributing to the mishap are noted and potential causal factors have been

identified. The detailed decomposition of mishaps #1–4 utilizing the approach described above can be found in corresponding appendices at the end of this document.

A detailed review of a mishap sequence allows for the identification of the potential failure events. Subsequent fault trees, as shown below, are constructed linking all the origins of the failure event to the casual factor that lead to the mishap. These causal factors shall be considered the root causes of the mishap.

1. Failure event—Larger than normal intake of water
    a. Wave and wind water lapping into the exposed starboard electric bilge outlet
        i. Uncontrolled contact with well deck resulting in damage to starboard electrical bilge outlet
            1. Unknown engine stall on stern gate
            2. Inability to restart the engine
                a. Discharged battery bank
                    i. Generator failure
                        1. Water intrusion from missing bolts
                            a. Poor quality control/maintenance operations.
                            b. Failure to conduct pre-operations check/pre-water operations check.
2. Failure event—Larger than normal intake of water
    a. The holes from the missing bolts on the plenum housing and cargo hatch
        i. Poor quality control/maintenance operations.
        ii. Failure to conduct pre-operations check/pre-water operations check.
3. Failure event—Larger than normal intake of water Causal Factor
    a. Exhaust grill and plenum housing not properly secured.

i. Poor quality control/maintenance operations.

ii. Failure to conduct pre-operations check/pre-water operations check.

4. Failure event—Larger than normal intake of water

    a. Degraded electric bilge capacity

        i. Discharged battery bank

            1. Generator failure

                a. Water intrusion from missing bolts

                    i. Poor quality control/maintenance operations.

                    ii. Failure to conduct pre-operations check/pre-water operations check.

5. Failure event—Larger than normal intake of water

    a. No hydraulic bilge capacity

        i. Unknown engine stall on stern gate

        ii. Inability to restart the engine

            1. Discharged battery bank

                a. Generator failure

                    i. Water intrusion from missing bolts

                        1. Poor quality control/maintenance operations.

                        2. Failure to conduct pre-operations check/pre-water operations check.

D. SUMMARY

The process of decomposing has been repeated for each mishap. The four examined mishaps have the same end state: the vehicle submerges/sinks. There are several similar

failure events that are also common across the mishaps. These failure events often shared the same casual factor origins. For example:

- poor quality control during maintenance operations
- failure to conduct pre-operations check/pre-water operations check

Each of these mishaps shares a common human related casual factor, human error, or violation. Human error can be further characterized as either skill-based, judgement, or misperception (DoN 2005). The AAV relies heavily on policy and procedures to mitigate known hazards but current safety assessment state of practice for the AAV does not acknowledge human error or violation as a casual factor. Additionally, each of the identified hazards is treated as independent from one another. There is no relation or dependency considered between one hazard being realized and its subsequent effect of triggering additional conditions. It is the view of the author that the current safety assessment state of practice for the AAV is insufficient and a method that supports a comprehensive assessment of various end states as derived from the various sequence of basic events to include human related causal factors is needed.

IV. METHODOLOGY

The intent of this research is to identify a method for legacy system managers to close the gap between the risks that are formally identified using methods such as MIL-STD-882E mishaps that occur during system operation. Mishap scenario models built by dissecting the system mishap reports are a core component of the method proposed below. However, the method could be applied to a system anywhere in the systems engineering design process if there is sufficient data to construct applicable mishap scenario models. For example, operational concepts, architectural views, and historical data on similar in-service systems can be utilized to develop preliminary mishap scenario models for a developmental system. The fidelity of the mishap scenario models will increase as the system architecture is defined and the product baseline is developed, thus allowing the method to be applied through the design phase. While this method is adaptable anywhere along the design process, the proposed method is developed below as it applies to legacy systems, and specifically to the AAV and the associated mishaps previously discussed.

A. FRAMEWORK

The proposed method is in Figure 1.

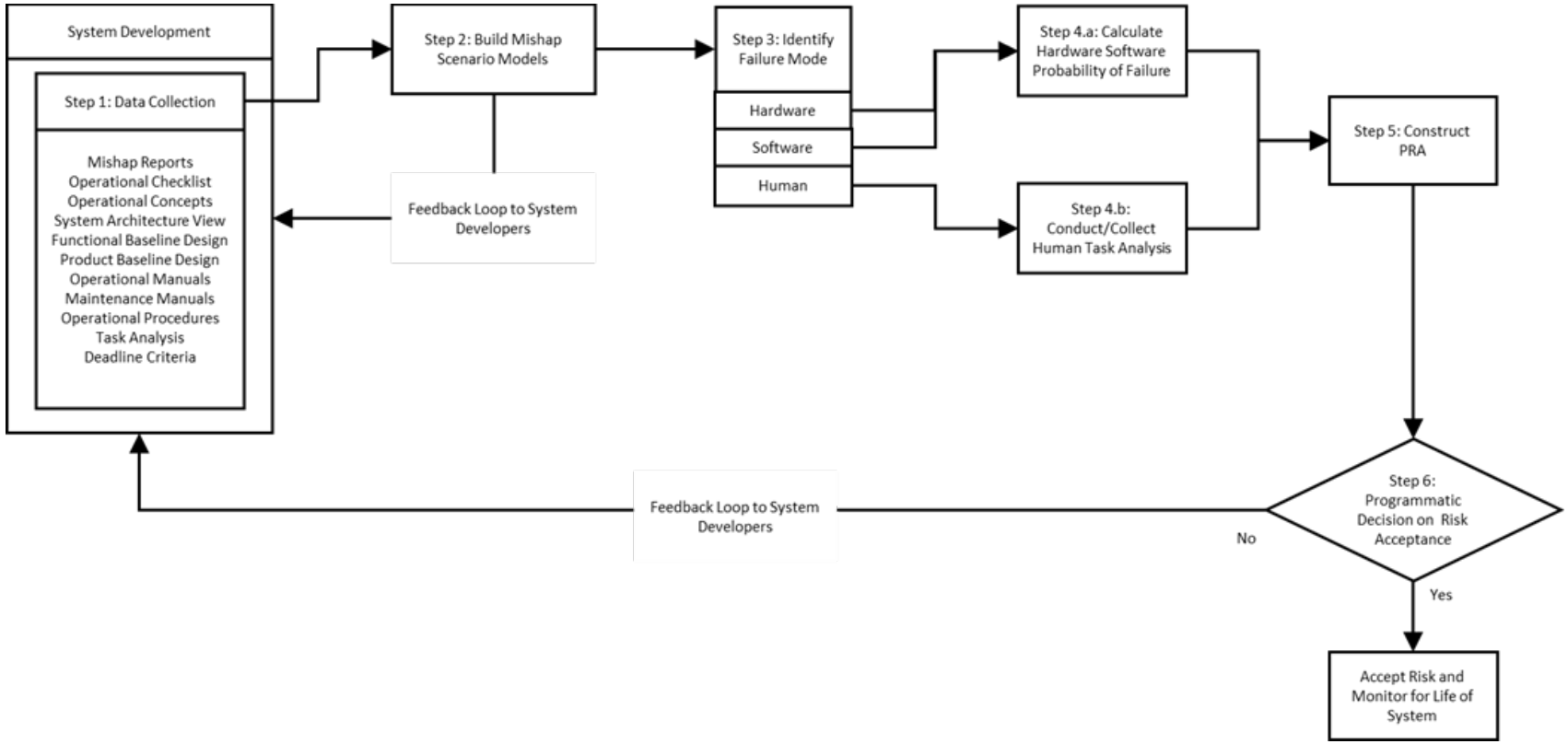

Figure 1. Mishap Assessment Method

To illustrate the application of the proposed method to the AAV within the previously defined scope of this research, the description of the application of the method will be described as only addressing mishap #2. The application of the method to the mishap #1, mishap #3, and mishap #4 can be found in each corresponding appendix at the end of this document.

1. Step 1: Data Collection

The development of mishap scenario models is the core component of this method. The fidelity of the developed mishap scenario models is dependent on the quality of the documentation collected. Mishap reports, operational checklists, operational tasks, and procedures need to be collected. As previously noted, the AAV is currently in service in the military. Data collection for in service equipment can lead to information overload. The primary focus of the method presented here for the AAV is to quantify the actual risk of the system, thus the primary data collection focuses on the mishap report and pre-water operations checklists.

2. Step 2: Mishap Scenario Models

The decomposition of the collected data is important to this step. Figure 2 illustrates a constructed mishap scenario of mishap #2. The mishap scenario development follows the mishap report decomposition process described in Section 3.C. This mishap scenario is a graphical depiction of the key elements identified from the decomposition that led to the mishap.

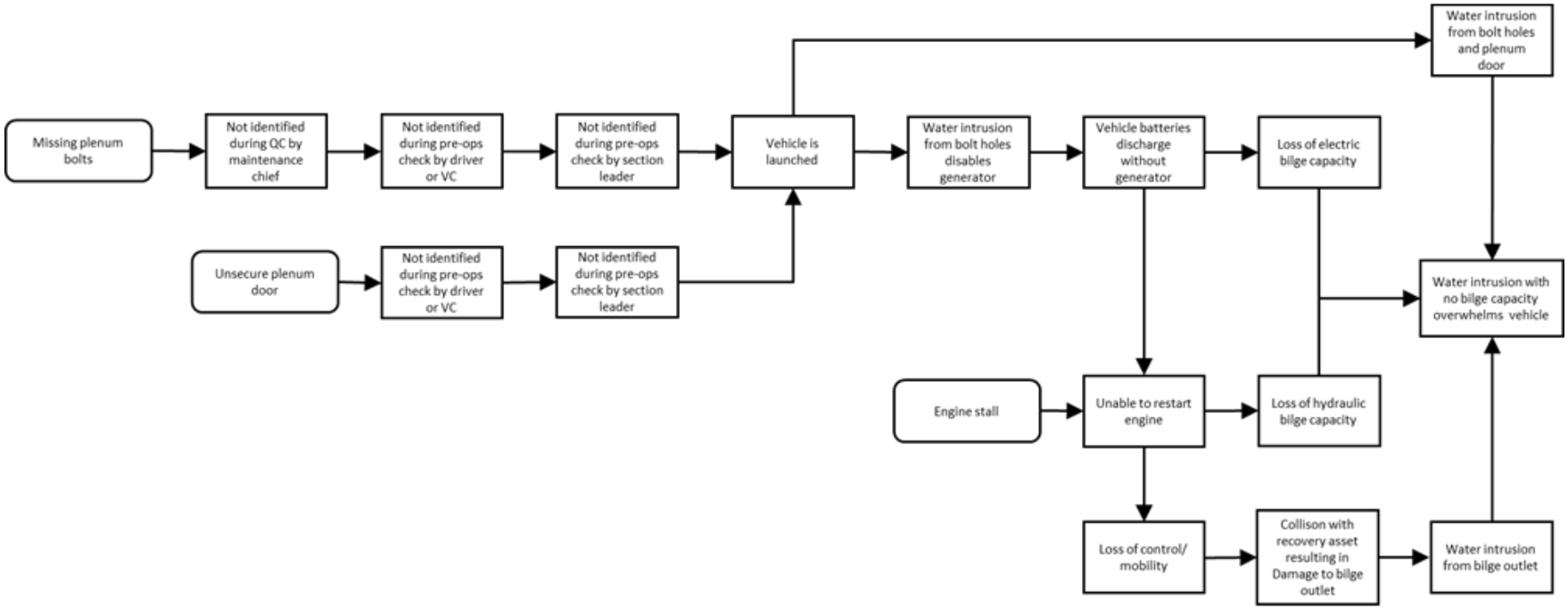

Figure 2. Mishap #2 Scenario

3. Step 3: Identify Failure Modes

The mishap scenario models lay out the events in the mishap report in a logical block flow diagram that allows for the identification of the contributing failure events. Once the failure modes are identified, corresponding fault trees and event trees should be constructed. The fault trees and events trees for this research are constructed in accordance with the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (Stamatelatos 2011). For this purpose, failure event shall be defined as the event that contributed to the mishap.

The author suggests that fault trees and event trees be constructed without probabilities. The intent is to focus on constructing complete logical fault paths. This is useful since the fault trees and event trees will likely be comprised of different combinations of the three types of failure events: hardware, software, and human that have substantially different means for determining the probability of failure. Computing or sourcing the related probabilities is addressed in later steps of the method. Figures 3 through 7 are the constructed fault trees and event tree for mishap #2.

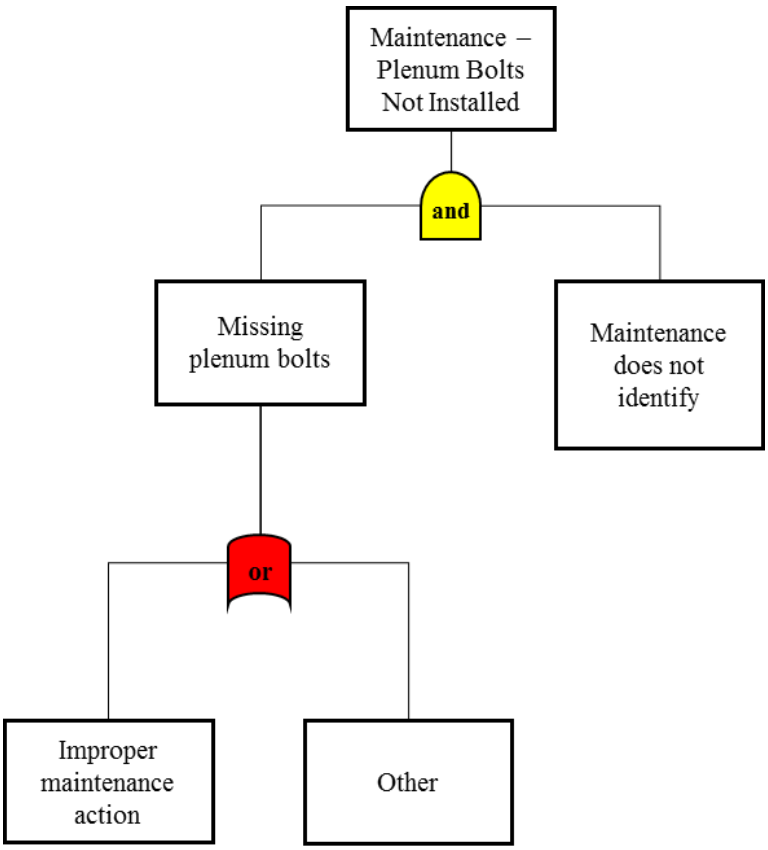

Figure 3. Maintenance—Plenum Bolts Not Installed FTA

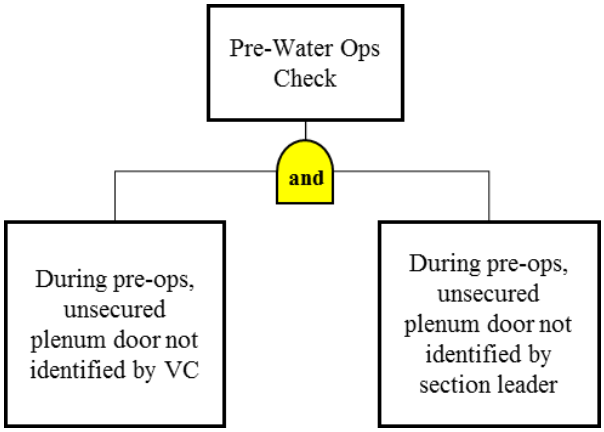

Figure 4. Pre-water Ops Check FTA

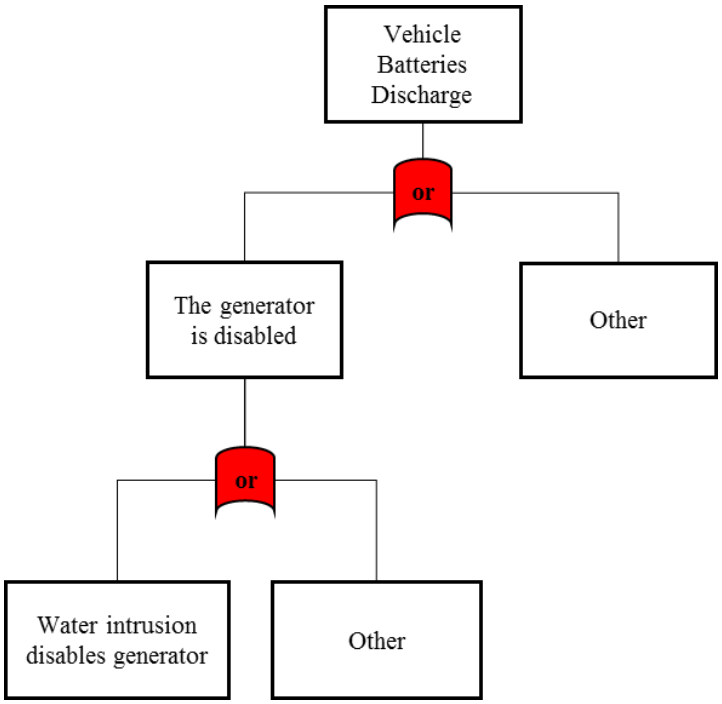

Figure 5. Vehicle Batteries Discharge FTA

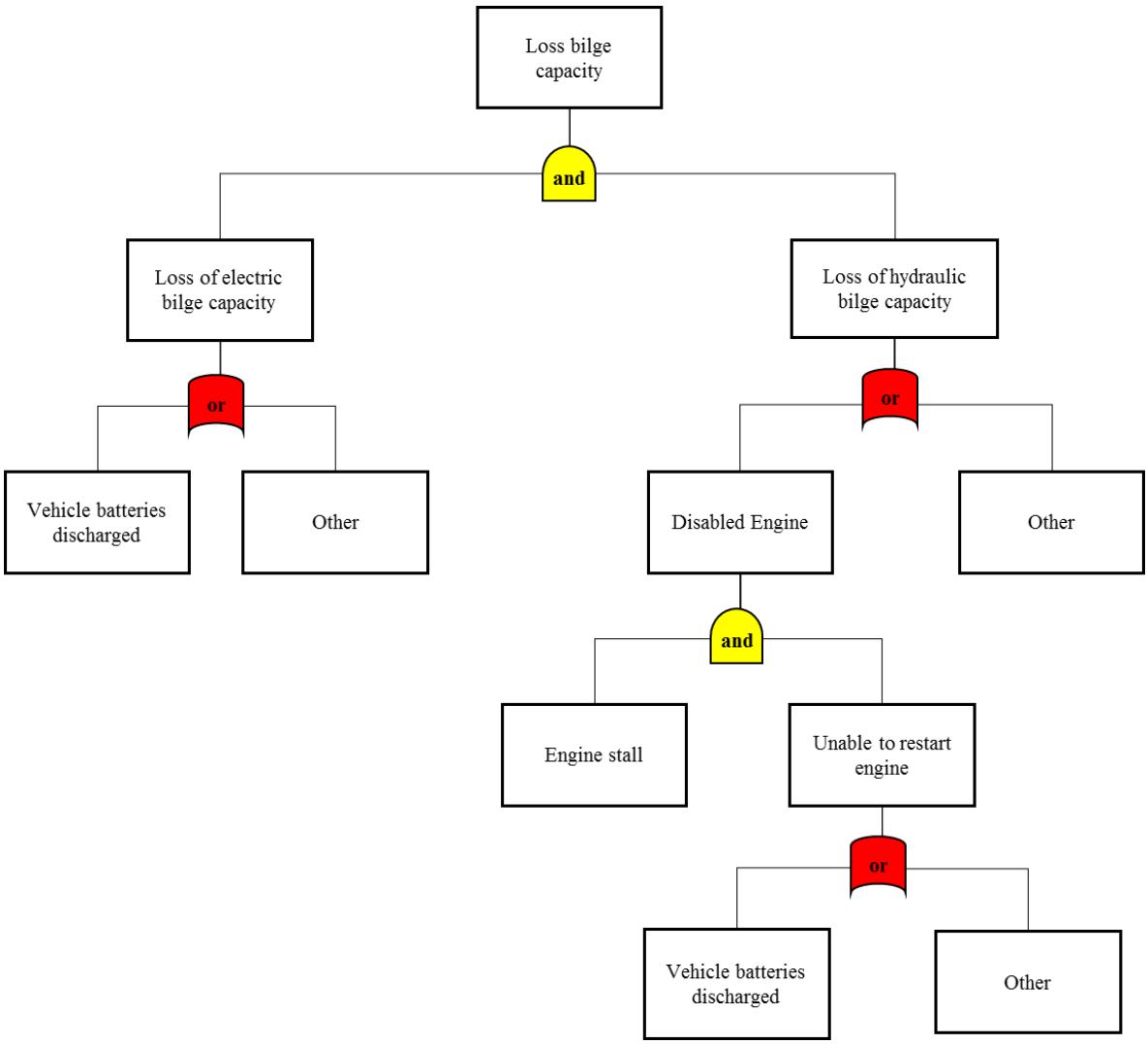

Figure 6. Loss of Bilge Capacity FTA

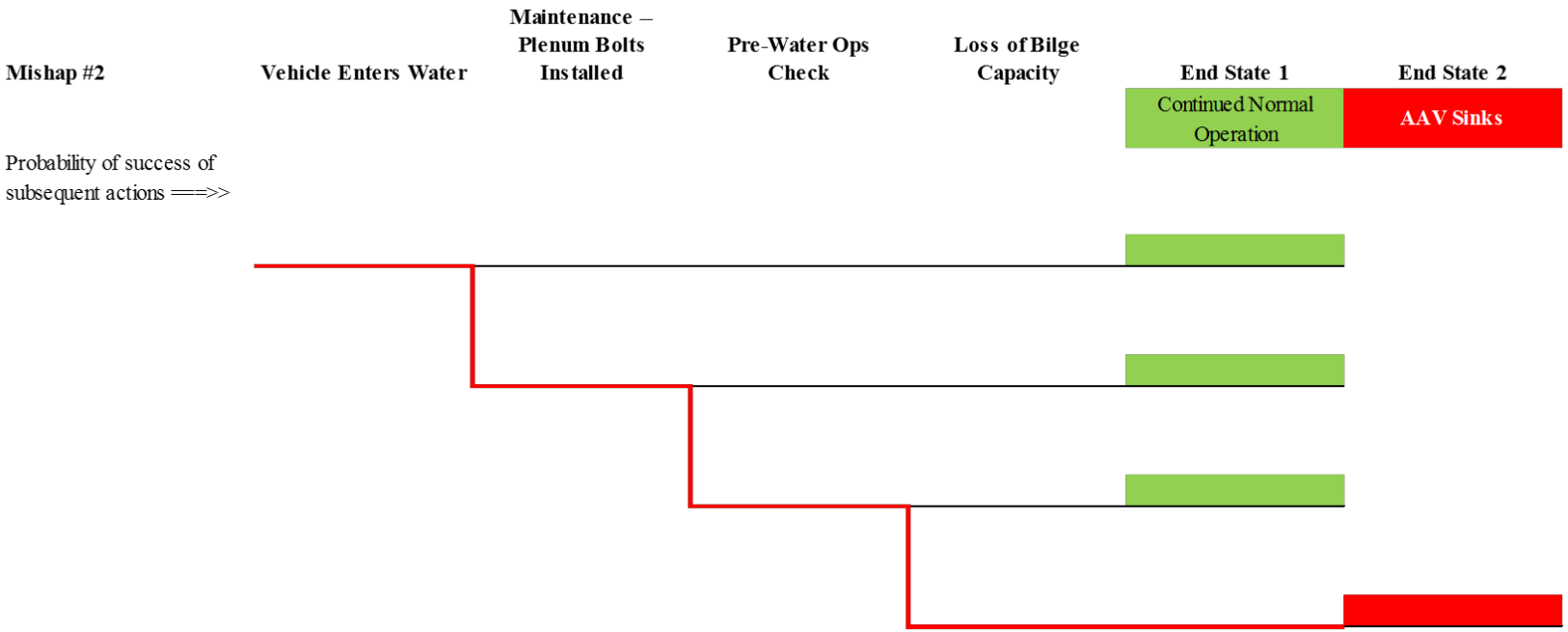

Figure 7. Mishap #2 Event Tree

4. Step 4.a: Calculate Hardware and Software Probability of Failure Distribution

Calculating the probability of the mishap is dependent on the ability to estimate the failure rate of those system components. Hardware and software failure probabilities are directly related to their reliability and should be extrapolated from reliability testing or documentation. In lieu of actual test data, the minimum reliability requirements for the subsystem or components can be utilized. The minimum reliability for the subsystem or components can be identified in the system specifications. A standard minimum reliability of 0.95 is utilized in this paper to calculate the failure probability of all subsystems and components identified. Note that the reliability data in this paper is intentionally not accurate AAV data and is for demonstration purposes only.

5. Step 4.b: Collect or Conduct Human Task Analyst

Human error probability is challenging to accurately determine. Human error is known to vary depending on the task, frequency, and environment (Stamatelatos 2011). This research advocates for human task analysis to be conducted in relation to the actions or activities required of the operator/maintainers leading to the mishap. This human task analysis will assist in identifying an appropriate HRA technique to determine an acceptable human error probability for the specific failure.

As previously stated there are numerous HRA modeling approaches, each with its own technique or guidance for quantifying the human error probability. THERP, CREAM, SPAR-H, and NARA are examples of acceptable techniques that are applicable to a variety of activities. Substantial resources and time would be required to specifically tailor an existing technique to the AAV operations, thus for the purposes of this research, the human error probabilities will be taken from NARA. NARA uses actual human error data and defines a set of generic tasks that can be generalized to match similar activities. For all practical purposes human error probability is the same as human unreliability. Table 2 is the list of NARA generic tasks utilized in this research.

Table 2. NARA Generic Task List. Source: Kirwan et al. (2005).

Generic Task	Nominal Human failure probability (5^{th}–95th percentile bounds)
(A) Totally unfamiliar, performed at speed with no real idea of likely consequences	0.55 (0.35–0.97)
(B) Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26 (0.14–0.42)
(C) Complex task requiring high level of comprehension and skill	0.16 (0.12–0.28)
(D) Fairly simple task performed rapidly or given scant attention	0.09 (0.06–0.13)
(E) Routine, highly practiced, rapid task involving relatively low level of skill	0.02 (0.007–0.045)
(F) Restore or shift a system to original or new state following procedures, with some checking	0.003 (0.0008–0.007)
(G) Completely familiar, well-designed, highly practiced, routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced personnel, with time to correct potential error, but without the benefit of significant job aids	0.0004 (0.00008–0.009)
(H) Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	0.00002 (0.000006–0.0009)

Utilizing NARA generic task human failure probability data is not optimal; however, it likely falls within an order of magnitude of reality and therefore is sufficient for demonstrating the proposed method. If the proposed method is used for a formal safety reassessment of the AAV, it may be useful to develop an HRA that is specifically suited for the AAV. For the purposes of this research, tasks such as routine crew checklist (Pre-ops and Pre-water Ops) and maintenance quality control checklists are identified as category (D) with a nominal human failure probability of 0.09 as a baseline. Each subsequent level of supervisor unreliability should be doubled if previous level failed. For example, the VC is the first level at 0.09. If VC fails, section leader unreliability will be 0.18. If section leader fails, the Splash Team Leader unreliability will be 0.36. It is useful

to note that the third level of supervision is a recent development to address previous failures and was not in place at time of the mishaps. For driver tasks, particularly student or novice drivers, the task is identified as category (A) with a nominal human failure probability of 0.55. Maintenance tasks (first echelon crew tasks and second echelon maintainer tasks) are identified as category (c) with a nominal human failure probability of .016.

6. Step 5: Conduct PRA

Conducting the PRA is basically finishing the previously constructed FTAs and ETAs using the probabilities from Step 4. For purposes of this paper, a PRA software tool called SAPHIRE was utilized. SAPHIRE was developed by the Idaho National Laboratory for the United States Nuclear Regulatory Commission. The FTAs and ETAs shown above and elsewhere in this document were developed in SAPHIRE which in turn provided probability calculations for each cut set. The use of SAPHIRE or a similar software package such as CAFTA is recommended to ensure the correctness of the calculations. Hand calculations are more prone to errors. Table 3 shows the top two cut sets related to mishap #2. A complete cut set for mishap #2 can be found in Appendix E.

Table 3. Mishap #2 Cut Set

#	Cases	Prob/Freq	Total %	Cut Sets	
1	C	1.00E-06	89.03	MISHAP_2: 4	
		1.00E+00		SPLASH	Vehicle enters the water (either from ship or shore)
		1.00E-01		ENGINE_STALL	Engine stalls
		1.00E+00		GENERATOR_DISABLED_WATER	Water intrusion disables generator. NOTE: This should be updated with probability of water intrusion for missing bolts
		1.00E-01		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.00E-02		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.00E-01		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.00E-01		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
2	C	1.00E-07	8.9	MISHAP_2: 4	
		1.00E+00		SPLASH	Vehicle enters the water (either from ship or shore)
		1.00E-03		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.00E-01		ENGINE_STALL	Engine stalls
		1.00E+00		GENERATOR_DISABLED_WATER	Water intrusion disables generator. NOTE: This should be updated with probability of water intrusion for missing bolts
		1.00E-01		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.00E-01		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.00E-01		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC

7. Step 6: Programmatic Decision on Risk Acceptance

This step is a management decision point on whether to accept the risk and seek formal acceptance per MIL-STD-882E or to direct resources to mitigate the risk. The details of such a decision can vary from organization to organization. The programmatic decision will be based on a specific organizational matrix weighing the value of the capability provided from the asset as is, the probability and severity of a mishap occurring, and the cost of fixing or mitigating the risk. The specifics of an organization's decision matrix are beyond the scope of this research. However, the implications of the identified risk will be briefly discussed here as it pertains to the organization's decision.

B. SUMMARY

As previously stated, the program office for AAV currently is aware of several hazards contributing to the sinking of the vehicle that have been previously accepted. These hazards are all assessed as 1E (catastrophic/remote) risks per MIL-STD-882E, meaning there is potential for loss of life with a probability less than 9.90E-7. Recall from above discussion that these risks were identified primarily from analysis techniques that focused on single-point failures with little to no consideration for the human element of the system. Thus, it is possible that a misleadingly low probability of a mishap being reported compared to the realized mishaps that are being observed in the AAV fleet. The results from the PRA conducted on the aforementioned mishaps provide a quantitative assessment of the chain of events that was specific to the operation of the system as designed that were not previously captured or acknowledged. Table 4 presents the specific probability in relation to the cut sets leading to the unwanted event of sinking an AAV as observed within the mishap reports. Note that this assessment is for demonstrational purposes only and the probabilities reported are intentionally and explicitly not accurate with reality.

Table 4. Mishap Probability Summary

Mishap	Cut Set	Probability	MIL-STD-882E Probability Category
#1		9.15E-02	B
#2		2.6472E-06	D
#3		2.09952E-06	D
#4		3.02E-04	D

Assuming the calculated probabilities are accepted to be within the acceptable order of magnitude and severity is accepted as catastrophic as is routinely acknowledged as the credible consequence of loss of life for mishaps related to sinking of a vehicle, these risks would be categorized as 1B, 1D, 1D, 1D respectively per MIL-STD-882E. These risks would then in turn be subjected to the same weighted organizational matrix based on value of the capability provided by the system as currently designed, the probability and severity of a mishap occurring, and the cost of fixing or mitigating the risk.

The decomposition of realized mishaps and the subsequent PRA of these mishaps suggest a greater probability of the mishaps that result in the sinking an AAV than previously acknowledged. Additionally, if this risk is deemed unacceptable, this quantitative assessment has identified high-risk events that program managers and systems engineers can focus resources to in support of improving safety.

THIS PAGE INTENTIONALLY LEFT BLANK

V. DISCUSSION

The method proposed and demonstrated above shows that there is a potentially significant difference between the acknowledged probability of potential mishaps and the quantified probability of actualized mishaps reported on AAVs. This is largely due to current focus of MIL-STD-882E on single failure events and the way the human element is ignored within the system during the safety assessment. The probability of a single-point failure leading to a sinking mishap is designed to be improbable within the system. However, as demonstrated by historical mishaps and the proposed method, the culmination of several failures linked in a sequence of causal factors has a considerably higher probability of leading to a mishap. When the human failure probability is included in the equation that probability increases further. The current approach in MIL-STD-882E can lead program managers to unwittingly expose the warfighter to a system that is not as safe as managers believe. The method proposed in this research presents a more accurate and quantifiable probability of a mishap that decision makers can take action to address rather than ignore.

This method could be applied to a system anywhere in the systems engineering design process if there is sufficient data to construct applicable mishap scenario models. For example, operational concepts, architectural views, and historical data on similar in-service systems can be utilized to develop preliminary mishap scenario models for a developmental system. The fidelity of the mishap scenario models will increase as the system architecture is defined and the product baseline is developed, thus allowing the method to be applied through the design phase. Early implementation of this method will allow stakeholders to focus resources in support of improving the safety of their system while still in the design phase.

Once the proposed method is implemented, the results must be captured and reported in such a manner that allows program managers and system engineers to address the mishap. The current focus on hazards within MIL-STD-882E drives the reporting of risks in relation to the probability of a single failure event leading to a mishap. This is a singular relationship that does not include the sequence of failure events that often leads to

a mishap as illustrated in real-world mishap reports. An inclusive holistic approach of reporting the probability of the mishap occurring regardless of the complexity of its failure event chain must be included. The cut sets produced from the application are a key element in creating an all-inclusive risk reporting approach. The cut sets capture all of the parallel pathways that can lead to the mishap and each cut set is a specific sequence of failure events leading to the mishap. These cut sets can be identified, reported, and tracked within the parameters of MIL-STD-882E HTS.

There are noted limitations with the proposed method, notably with the utilization of the NARA generic task list for determining the human error probability. In an ideal situation, resources would be tasked to further quantify the probability of human failure probability specific to the AAV community. However, there may also be cultural impacts within that same community dependent on command climate and leadership that could create variation between different groups of AAV users. While the utilization of the NARA generic task list probabilities satisfies its purpose in this research for demonstrational purposes, it is believed to only be within an order of magnitude of reality. The use of the NARA task list probabilities may be optimistic in comparison to a specific HRA for the AAV community considering the vast difference between a military occupation specialty and nuclear reactor personnel, and their operating environments.

VI. CONCLUSION

The risks associated with the equipment provided to the warfighter are often articulated and acknowledged quite differently from the risks realized during operation. MIL-STD-882E focuses on single-point failures but does not generally include failure modes that require sequential failure events to occur. However, this approach ignores the realization of mishaps from multiple system failure events to include the human events. This situation presents the risk of a mishap occurring much lower than as observed with the AAV fleet. For example, the current risk assessment methodology from MIL-STD-882E identifies the probability of sinking an AAV as improbable, despite the fact that several vehicles have been sunk during the course of their operation.

Real world AAV mishaps were analyzed to identify failure events, casual factors, root causes, and trends that lead to the mishaps occurring. Various risk assessment methodologies were reviewed and the PRA method of risk assessment was selected for use because it showed the most potential in correcting the deficiency between the acknowledged risk and the actual risk as observed from AAV operations. The development of a PRA- based method specific to the operational scenarios of the AAV system and the decomposed mishap reports allowed the observed risk to be accurately quantified and reported. The proposed method demonstrates that there is a potentially significant difference between the acknowledged probability of potential mishaps and the quantified probability of actualized mishaps reported. This is largely due to the current focus on single failure events and the way the human failure probability is ignored within the system.

The implementation of this method will more accurately inform stakeholders of the current risks of their equipment as designed and operated, and allows stakeholders to focus resources in support of improving the safety of their system.

There are several areas of future work that should be considered in regards to this research. In addition to a specific HRA directly applicable to the AAV, more detailed probabilistic assessments will be embedded into the method. Once the quantification of the HRA aspect of the proposed method is refined, this methodology should be applied across

the full operational profile of the AAV. Subsequently, there are plans to apply this method to the next generation amphibious vehicle.

APPENDIX A. MISHAP #1

A. MISHAP #1 DECOMPOSITION

The following is an example of the decomposition of mishap #1 utilizing the approach described earlier.

Est 0730–0800 pre-water operations check conducted on mishap vehicle the driver and crew chief.

Est 0850 vehicle commander reports to platoon Sgt that VEH#1 was prepared to launch. Platoon Sgt collects pre-water operations checklist/manifests and conducts water integrity check of all vehicles. VEH#1 three-member crew occupies the following stations: vehicle commander in turret, crew chief in Troop commander's (TC) station, driver in the driver's station.

Est 0855 on board VEH#1 vehicle commander directs driver to change mode selector switch from land mode to water/jets mode.

OD)2) Crew chiefs, platoon sergeants, platoon commanders do not ensure the drivers employ the bow plane each time the AAV is waterborne in accordance with operator's manual TM 09674A-10/3. Interviews with driver, crew chief, platoon sergeant, and platoon commander indicated that deploying bow planes are up to individual preference and its use is not universally accepted among AAV supervisors.

0900 vehicles begin launch.

Est 0902 VEH#1 prepares to launch, driver places gear selector in first gear, releases brake, gets green flag, fully depresses accelerator pedal, VEH#1 splashes and surfaces uneventfully.

Est 0903 (the following sequence of events occur within an estimated 45 seconds onboard VEH#1)

-Driver turns on electric bilge pumps,

-Driver places vehicle gear selector in neutral position while accelerator pedal is completely depressed

-Driver pushes hand throttle all the way forward and removes foot from accelerator pedal.

O1)A) Operator's Manual TM 09674a-10/3 Assault Amphibious Vehicle lacks guidance on use of hand throttle control

OA1) supervisory/training - driver was unfamiliar with the safe waterborne operation of an AAV. The driver was never trained in the use of the hand throttle in waterborne operations, had never used it to move an AAV but chose to use the hand throttle to control the speed of VEH#1 once waterborne

-Driver unlocks and opens his hatch, stands on driver's seat, turns body in a clockwise direction until facing aft in an attempt to secure his hatch in the open position. Vehicle commander and crew chief facing aft locking their hatches simultaneously with driver.

O2)C) 2D AA BN Order P3000.2d Standard Operating Procedures for AAV Operations lacks guidance on when to safely open hatches when AAV becomes waterborne.

01)B) Operator's Manual TM 09674a-10/3 Assault Amphibious Vehicle lacks guidance on when to safely open hatches when an AAV is waterborne and not employing the bow plane. The following paragraph is an excerpt from the Assault Amphibian School student handout on driving in water. (This handout is dated Jan 92 and references tm 07007b-10 which is now replaced by TM 09674A-10/3). "Without the bow plane modification, an empty AAVP7A1 assumes a nose-down attitude which is aggravated as water speed increases. When engine speed exceeds xxxx rpms, the situation becomes critical and all hatches must be closed to prevent an excessive amount of water from entering the vehicle. After the hatches are closed, the nose-down attitude causes water to pour over the vision blocks obscuring the driver's visibility and diminishing his ability to operate the vehicle. To regain visibility the driver must significantly reduce the vehicles forward speed. When the bow Plane is extended (raised), this prevents the vehicle from

assuming the bow-down attitude allowing the driver and others a better operational field of vision. In higher sea states the bow plane effectiveness increases" (USMC 2012).

-At this time driver experiences difficulty in securing hatch due to missing driver's hatch support.

OH1) Driver's hatch support which stops the hatch from impacting the rear plenum and aligns hatch and locking notch in the fully open position was missing from VEH#1. If hatch support was in place driver would not have spent 3–4 seconds attempting to secure his hatch in fully open position.

-Vehicle commander turns forward and notices water up to driver's hatch and warns via intercom that driver is about to get wet.

-Driver turns forward just as water begins rushing into driver's hatch

-Driver turns counterclockwise and throws hands in the air, faces towards crew chief in TC with a look of panic and Confusion.

-Vehicle commander directs driver via intercom to pull the hand throttle back.

-Upon hearing vehicle commander's direction crew chief drops down his hatch to the interior of VEH#1 and moves forward in an attempt to reach the hand throttle but is unsuccessful due to the volume of water rushing in through driver's hatch.

-While climbing out of the TC hatch, crew chief hears vehicle commander frantically shout to kill the fuel, shut it down via intercom.

-Crew chief exits TC hatch moves forward arriving adjacent to drivers hatch in an attempt to reach hand throttle from the top but this was also unsuccessful because the driver's hatch was now submerged below the water line as the vehicle was submerging with a heavy forward port list.

-VEH#1 submerges completely

B. MISHAP #1 MISHAP SCENARIO MODEL

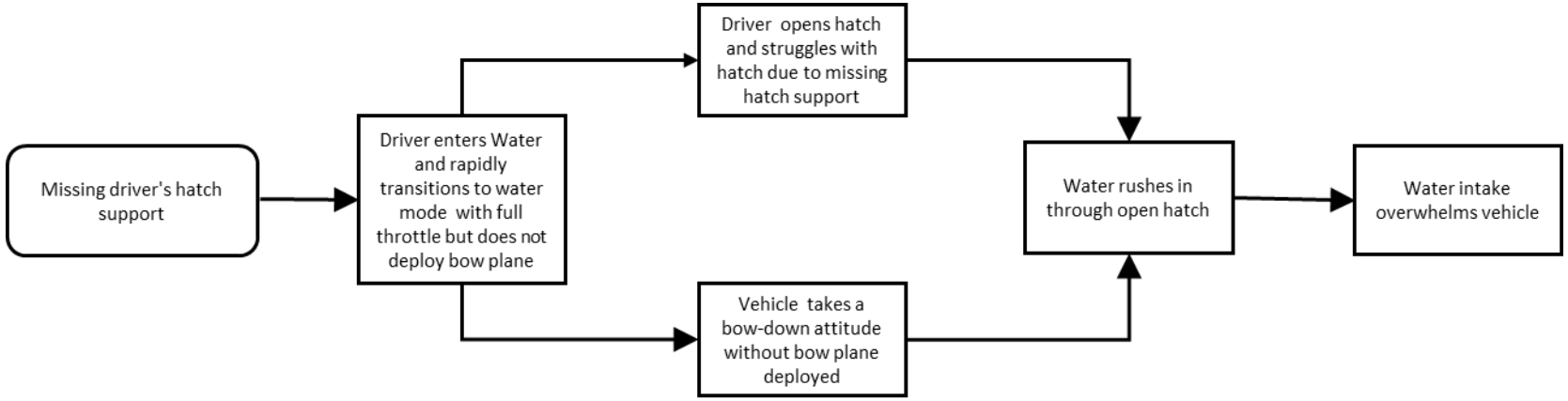

Figure 8. Mishap #2 Scenario

C. MISHAP #1 FAILURE MODES

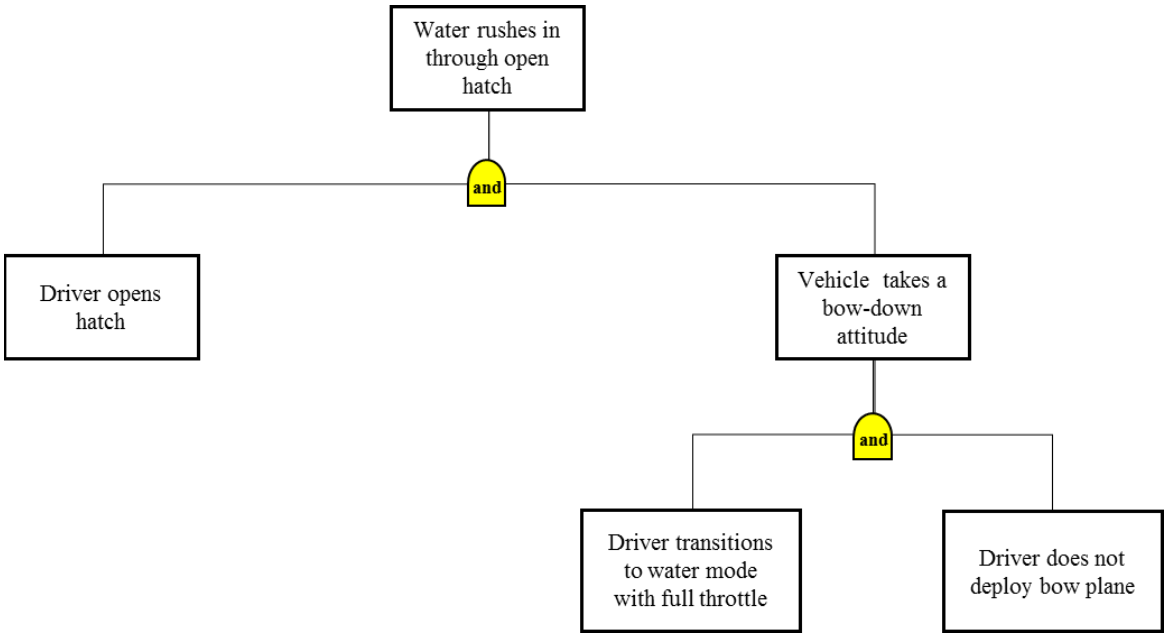

Figure 9. Operation—Water Rushes in through Open Hatch

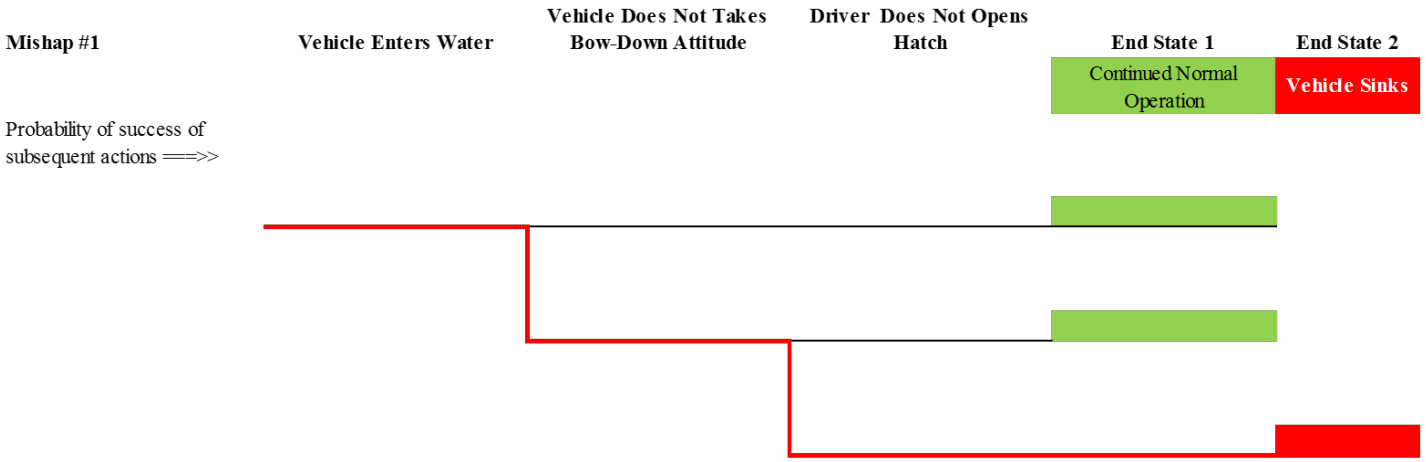

Figure 10. Mishap #1 Event Tree

APPENDIX B. MISHAP #2 DECOMPOSITION

The following is an example of the decomposition of mishap #2 utilizing the approach described earlier.

P173. Vehicle (VEH) #1's pre-water operations checklist was not filled in on page I-4, which included battery volt indicator readings.

P174. VEH #1's pre-water operation checklist has the VC's initials next to the inspection line indicating that the exhaust grill lugs were serviceable without remarks and the VC claims to have personally inspected both lugs.

O3. VC did not check the rear exhaust locking lugs during the pre-water operations checks on 20 April 2009. The pre-water operations checklist was inaccurately recorded by the VC regarding the status of the exhaust grill locking lugs.

R118. The recovery divers confirmed the forward plenum lock indicator "Mushroom" was in the closed and locked position, the forward plenum dogs were closed, but not entirely into the fully locked position prior to recovery.

P175. VEH #1's pre-water operations checklist has the VC's initials next to the inspection line indicating that the heater exhaust outlet was closed and that the VC claims to have personally inspected the heater exhaust outlet.

R122.g. The Troop Heater vent was in an unlocked and open position.

O6. The VC did not secure the personnel heater vent during the pre-water operations checks and the pre-water operations checklist was inaccurately recorded by the VC regarding the status of the personnel heater vent.

E8. As VEH #1 first touched the stern gate of the ship, the engine quit and VEH #1 went dead in the water.

E13. Immediate attempts by the driver to restart VEH #1 failed.

E14. The battery bank was quickly tested by the CC and showed approximately 15.7 volts, well below that required to turn over the engine and restart VEH #1.

O12. The cause of the engine failure cannot be proven, but the inability to restart the engine was a function of a discharged battery bank.

O13. The cause of the discharged battery bank was most likely the result of a generator that was not providing enough power to the vehicle during the initial transit from the beach to the ship.

O14. The cause of the generator failure cannot be proven. Failure of the crew to properly secure the plenum housing and exhaust grill could have caused excessive leaking from waves and wind during the transit that dripped down onto the generator. However, the failure rate of that particular generator series and the history of electrical problems with that particular vehicle also provide a reasonably likely cause for the generator failure.

E15. When the engine quit, the mechanical bilge pumps ceased functioning, and the capacity for VEH #1 to pump out water was reduced.

O10. The electric bilge pumps were virtually ineffective after the initial loss of engine power. The combination of CC's testimony that he could not hear them operating as he normally could along with the very low voltage readings taken immediately after the engine died are strong indicators.

E20. After the engine quit, VEH #1 rotated 90 degrees counterclockwise and floated into the well deck with the starboard track in the well deck and the port track over the stern gate.

E21. Over the next 5–10 minutes, the wave action in the well deck moved VEH #1 at first toward the starboard side of the well deck without contact, and then to the port side and aft off the port quarter.

E22. The crew of VEH #1 felt jarring and impact with the ship but could not locate what it was hitting because the hatches were closed and they were working internally to the vehicle to trouble shoot restarting the engine.

R122.e. The starboard forward bilge outlet cover/ballistic cover assembly missing as well as damage to the armor plating mounting hardware near the bilge outlet.

O8. The starboard electric bilge outlet cover and the adjacent armor was damaged sometime after splashing, and before coming to rest on the ocean floor. It is inconceivable that the crew/section leader/splash team leader would have missed this damage in checking the bilge outlets as part of the pre-water operations checks, and there is no evidence that it was damaged by the divers or by the careful recovery.

O9. The most likely cause of damage to the starboard electrical bilge outlet and adjacent armor was rubbing on the stern of the ship by wave action in the well deck. The height of the stern gate dogs matches with height of the bilge outlet with VEH #1 under the wave action associated with the free surface effect of the well deck and could have easily "clipped" the ballistic cover of the bilge outlet. The stern gate corner could also have smashed the armor around the bilge outlet if not the bilge outlet itself. All witness saw VEH #1 getting bounced around in the well deck and as she floated out. Since no one was in position to see the actual impact, there is no testimony to prove this, but there is no otherwise reasonable explanation.

E39. The platoon sergeant made the decision to turn away VEH #2's first attempt to tow VEH #1 into the well deck because depth of water at the sill was only 4 feet, which was within the standard operating procedure (SOP) for both the ship and the AAV for regular recovery but was outside both Dock Landing Ship (LSD) and AAV SOP for recovery of a towed AAV.

E62. In the last 2–3 minutes as VEH #1 closes the 150–200m under tow to the ship's stern, the water level rises sharply.

E64. VEH #1 was riding noticeably lower in the water.

O15. The larger than normal intake of water (for the 35 minutes from the engine quitting until VEH #1's final approach was a combination of the standard leakage rate plus wave and wind water lapping into the exposed starboard electric bilge outlet, the holes from the missing bolts on the plenum housing and cargo hatch, and water leaking from the exhaust grill and plenum housing that was not properly secured.

O16. That the decisive moment occurred as VEH #2 turned for final approach and began towing VEH #1 into the wind and seas toward LSD. Seconds after turning toward

the ship, the starboard bilge drain submerged as a function of both the increased draft from the sea water taken on over the last 35 minutes, and the increased pressure on the bow from both wind and seas. Additionally, the strain of the tow lines several feet above the center of balance naturally created a bias toward a bow down tow.

E76. That as VEH #2 made contact with the stern gate and reached the sill a large wave hit VEH #1 and the first tow line parted.

E78. That VEH #2 was pulled backward slightly down the stern gate and within seconds the second tow line parted.

E79. That VEH #1 was well aft of the aft edge of the stern gate when both tow lines parted.

E80. That the bow of VEH #1 continued to rotate downward, and within 3–5 seconds the entire vehicle had submerged. The rapid timeline suggesting significant additional breaches of water tight integrity.

APPENDIX C. MISHAP #3

A. MISHAP #3 DECOMPOSITION

The following is an example of the decomposition of mishap #3 utilizing the approach described earlier.

M44. That VEH#1 was received by Assault Amphibian Schools Battalion on 3 Jan 2008.

M45. That the VEH#1 logbook did not show any hydraulic fluid loss since Jan 2010.

M46. That VEH#1 received an Annual Maintenance Inspection on 14 Sept 2009 that detected no discrepancies related to the plenum or hydraulic systems.

M47. That VEH#1 received a Semi-Annual Maintenance Inspection on 16 Mar 2010 that noted a hydro leak in the exhaust plenum.

M48. That VEH#1's exhaust Cam Lock was replaced on 3 Mar 2010.

M49. That a hydraulic leak in the plenums was repaired on 7 Jun 2010.

M50. That prior to going to the field the Sgt#2 believed the plenums worked correctly.

E8. That the Splash Team consisted of Sgt#3, Sgt#4, and SSgt#2.

E9. That a Pre-Water Operations Checklist was completed on VEH#1 as described in ref (d), prior to splashing into the ocean.

O2. That Pre-Water Operation Checklist and Splash Team Inspection procedures were followed as required in references (b) and (d).

E10. That the Splash Team inspected VEH#1 prior to launch and was found to be fully functional and watertight as described in ref (b).

E11. That the front plenum mushroom was up, indicating a closed intake plenum door, during both the Pre-Water Op and the Splash Team inspection.

T39. That when the plenum cylinder is fully extended but the cam lock is not mechanically locked, the mushroom is raised.

R26. That the MDSU1 photographs showed the front mushroom was down, indicating an open intake plenum door.

T37. That when the front plenum was raised the plenum door was open.

T38. That on 17 Jun 2010 the forward plenum of VEH#1 was tested by hooking it up to the hydraulic system of another AAV. The cylinder retracted and extended normally but the plenum doors did not mechanically lock. The test was repeated numerous times but the intake plenum cam lock never engaged.

T40. That on 17 Jun 2010 while testing the forward plenums, a hydraulic leak was detected on the rear plenum feed line.

O1. That VEH#1 sank due to rapid flooding caused by the intake plenum door opening in the surf zone. The plenum door opened due to the intake plenum door not being mechanically locked into place combined with a hydraulic leak from the rear plenum feed line.

E2. That the Sgt#1 was the crew chief of VEH#1 on the morning of 11 June and positioned in the Troop Commander seat when VEH#1 splashed.

E4. That PFC#1 was the driver of VEH#1 on the morning of 11 June.

E12. That VEH#1 took on water rapidly while nearing the end of the surf zone.

E14. That VEH#1 took a nose down angle and sank at the edge of the surf zone approximately 2–3 minutes after splashing.

E15. That Sgt#1 ordered the crew to escape as VEH#1 began to submerge.

E1. That VEH#1 sank during basic water training at approximately 0845, 11 June 2010 at approximate location MGRS 11S MS 580 811.

B. MISHAP #3 MISHAP SCENARIO MODEL

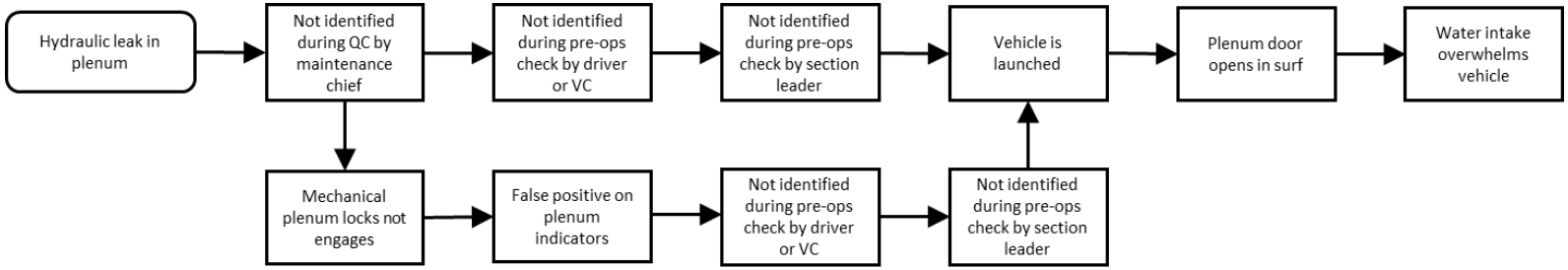

Figure 11. Mishap #3 Scenario

C. MISHAP #3 FAILURE MODES

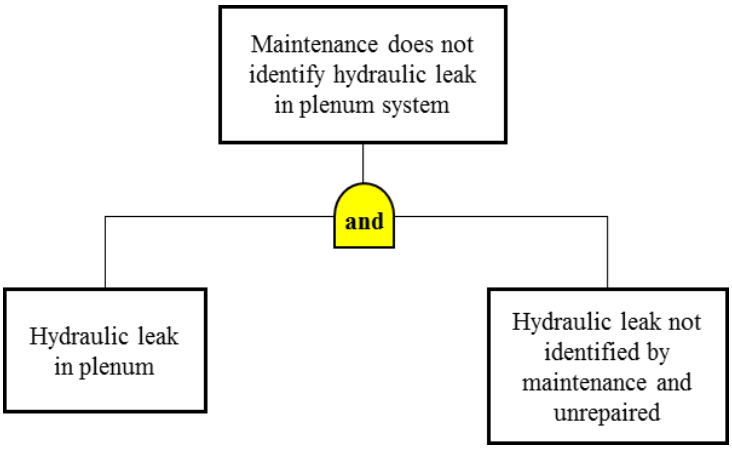

Figure 12. Maintenance—Hydraulic Leak Plenum

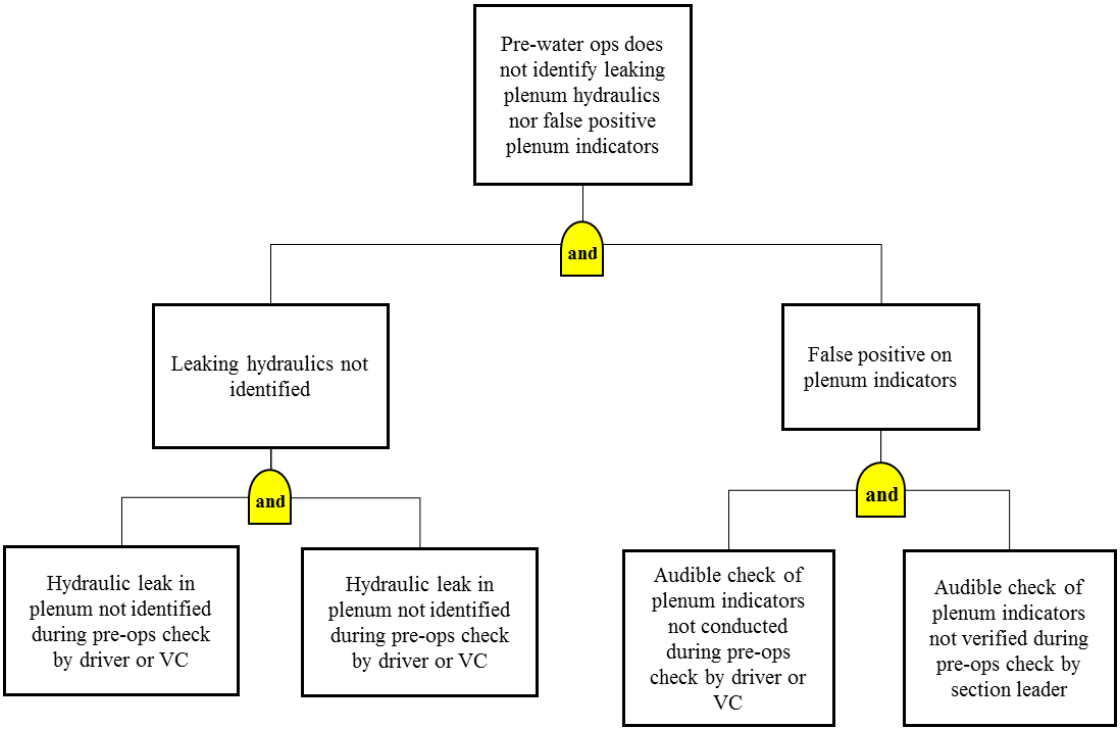

Figure 13. Pre-water Ops—Plenum

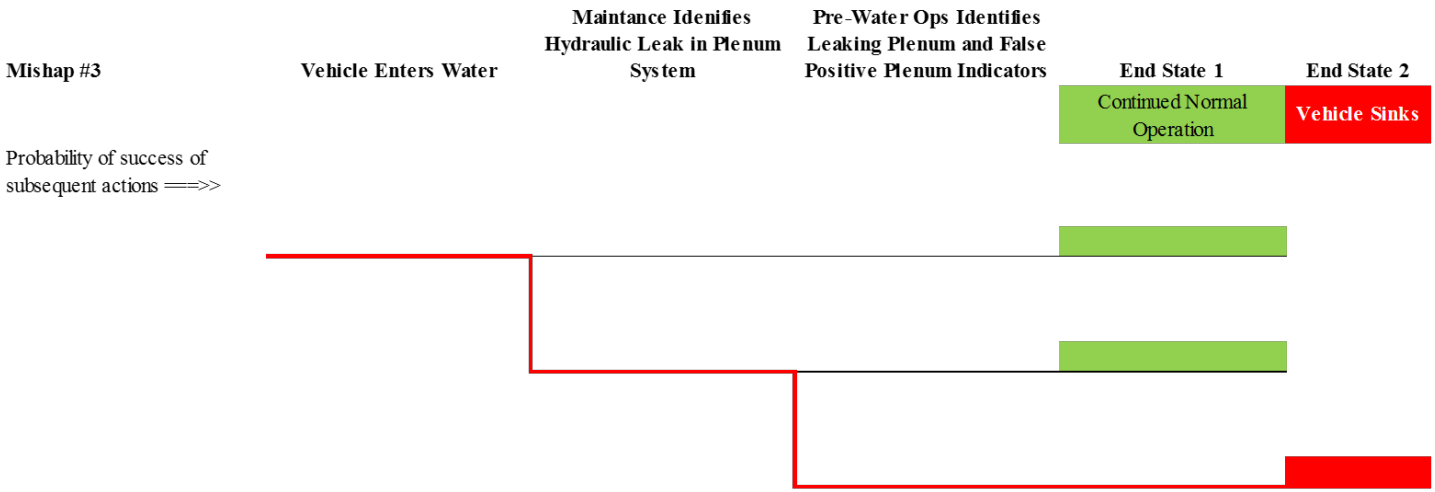

Figure 14. Mishap #3 Event Tree.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. MISHAP #4

A. MISHAP #4 DECOMPOSITION

The following is an example of the decomposition of mishap #4 utilizing the approach described earlier.

M10. A sticking throttle pedal on VEH#1 was first identified as early as late October 2010, but not reported by Sgt#1 the assigned crew chief.

M13. PMCS was conducted Monday, 10 January as per the detailed training schedule.

M17. Deadlining discrepancies for VEH#1 were annotated on the open ERO during the weekly MMO maintenance reconciliation on 11 January 2011 but were not formally identified as deadlining.

M18. A Limited Technical Inspection (LTI) was conducted on VEH#1 in conjunction with the Semi-Annual Service on 11 January 2011.

M19. In conjunction with the Semi-Annual service, a Communications LTI was conducted on VEH#1's communication suite on 11 January 2011. The inter-communication system was deemed functional.

M21. Deadlining discrepancies were annotated on semi-annual service on 11 January 2011 but were not identified as deadlining discrepancies.

M23. Sgt#2 knowingly falsified VEH#1's pre-operational check sheet, on 11 January 2011, for operations to be conducted two days later, on 13 January 2011; specifically block 5–1 vehicle internal communications.

M32. Although parts for deadlining discrepancies were on hand, the discrepancies annotated on the Semi-Annual service and maintenance reconciliation ERO, were not repaired prior to 13 January 2011.

M34. Sgt#3 repaired VEH#1's Lock-out linkage on 13 January 2011 after the land driving portion. This was identified to him by Sgt#2 as a sluggish engine. He found the

lock-out linkage disconnected and reconnected it. The repair was not directed to the sticking throttle pedal. Sgt#2's Testimony "it didn't feel like it wasn't getting enough power, it wasn't getting enough gas. When I was driving around, it felt like it was running a little sluggish."

M35. Although not part of a pre-operational check list, VEH#1's throttle pedal was operating in a degraded status (sticking) on 13 January 2011 during the land driving portion of the POI and was accepted by Sgt#2 as operational. Sgt#2's Testimony wasn't necessarily worried about the sticking of the throttle pedal, "I was more worried about the sluggishness of the vehicle."

P36. Intercom communications were not established in the vehicle Commander's position (turret) or rear crewman stations on 13 January 2011. Intercom Communications only existed between the Driver and the Troop Commander's station on 13 January 2011.

P38. The instructor crew on board VEH#1 did not report the degraded status of the vehicle's sticking throttle pedal or lack of intercom communications capability from the turret or rear crewman positions to the appropriate Maintenance personnel or Chain of Command on 13 January 2011.

P50. Sgt#4 was the crew chief of VEH#1 and signed the Pre-operations checklist on 14 January 2011.

P53. Sgt#4 signed VEH#1's pre-operations check sheet, for water operations, specifically block 18 vehicle internal communications as serviceable although no communication in the turret or rear crewman station were established.

P55. Each student who operated VEH#1 was briefed to the fact that the throttle pedal on VEH#1 was sticking, and they were briefed (informal training) on how to apply the heal toe method for manipulating the throttle pedal in order to manually correct the sticking throttle pedal.

P56. The instructor crew on board VEH#1 did not report the degraded status of the vehicle's sticking throttle pedal or the lack of intercom communications capability from

the turret or rear crewman positions to the appropriate Maintenance personnel or Chain of Command on 14 January 2011.

The Sinking

E64. The crew actions from the splash of VEH#1 through the conduct of the water driving course to the surfacing of the Marines are listed in sequence below.

- Splash procedures were conducted prior to launch.
- PVT#1 receives instruction to place the vehicle in 2nd gear from Sgt#5.
- PVT#1 begins moving vehicle down the ramp of the west rain room.
- The vehicle hits the water and begins floating.
- PVT#1 places the gear selector into the neutral position.
- Sgt#5 instructs PVT#1 to open his hatch.
- Sgt#5 instructs PVT#1 to drive straight out from the rain room for an unknown distance and to cross steer the vehicle.
- Sgt#5 instructs PVT#1 to conduct a port 360-degree turn.
- As the port 360-degree turn is completed, Sgt#5 instructs PVT#1 to drive towards the School house, while cross steering.
- PVT#1 starts driving towards the School house while cross steering.
- At some point, PVT#1 stops cross steering.
- Sgt#5 notices water level starting to rise over the bow of the vehicle and instructs PVT#1 to let off the throttle and to keep cross steering.
- Water rises to the point at which it starts to flow into the driver's hatch.
- Sgt#5 begins to yell louder at PVT#1 to get the throttle unstuck or turn off the fuel lever.
- PVT#1 attempts to kick the throttle pedal. Engine RPM's remain high.

- Sgt#2 squats down in the turret and yells to Sgt#4 to get students to a hatch and shut off the fuel lever.
- PVT#1 stands up, turns 45 degrees and looks at Sgt#5. Sgt#5's testimony "At that point, PVR#1 stood up and did about a half body turn and turned his head all the way around and looked at me with a look of sheer terror."
- PVT#1 becomes unresponsive to Sgt#5's commands.
- Water begins pouring in driver's hatch.
- Sgt#2 raises back up and sees driver's station completely under water.
- Vehicle submerges.

B. MISHAP #4 MISHAP SCENARIO MODEL

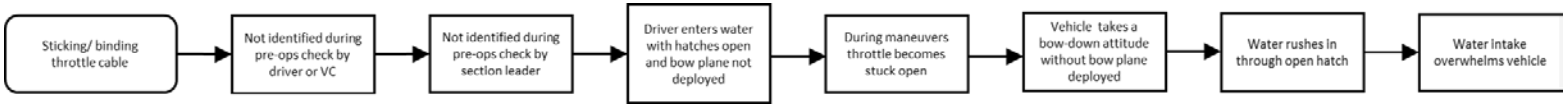

Figure 15. Mishap #4 Scenario.

C. MISHAP #4 FAILURE MODES

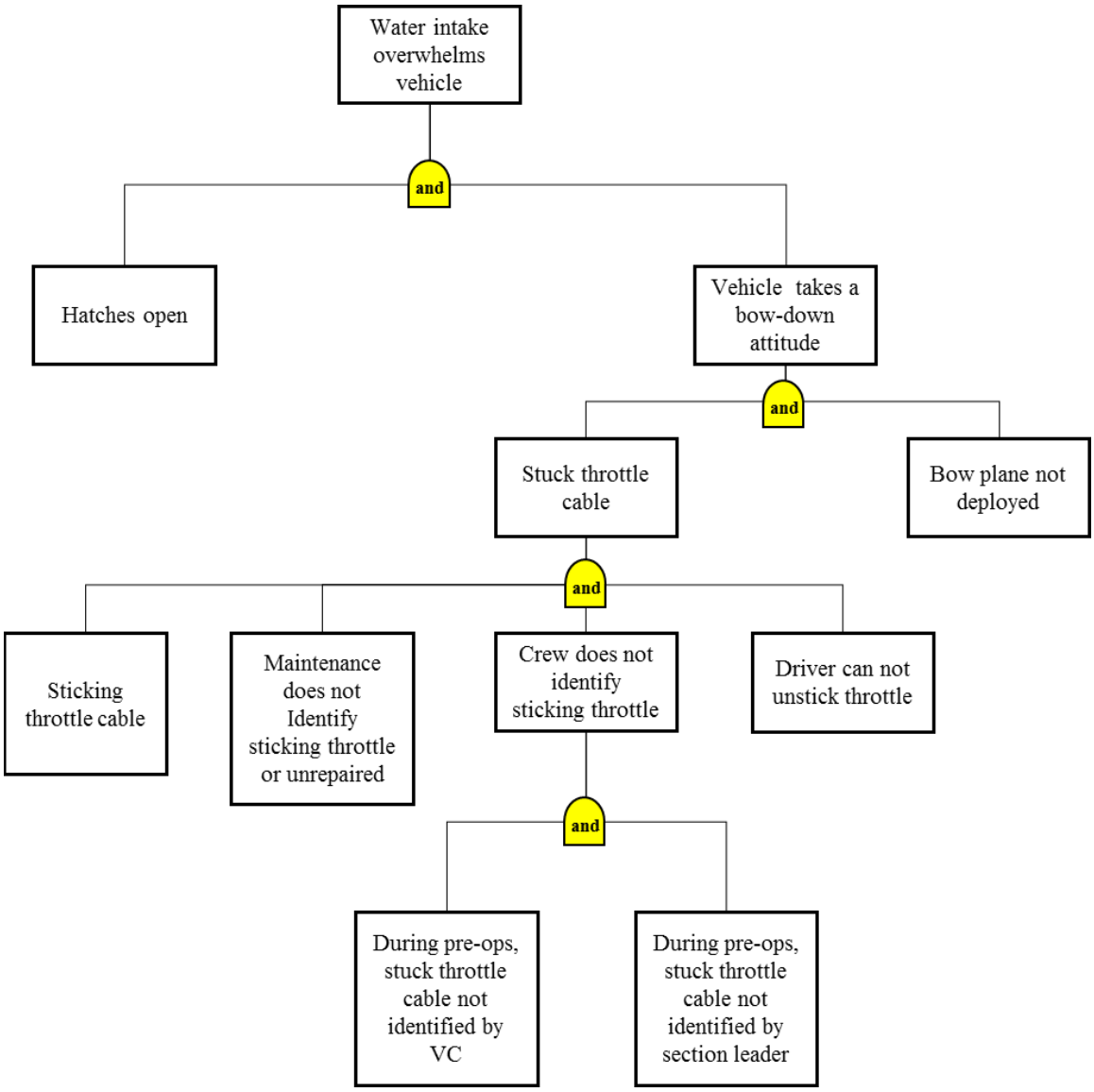

Figure 16. Operation—Water Rushes in through Open Hatch

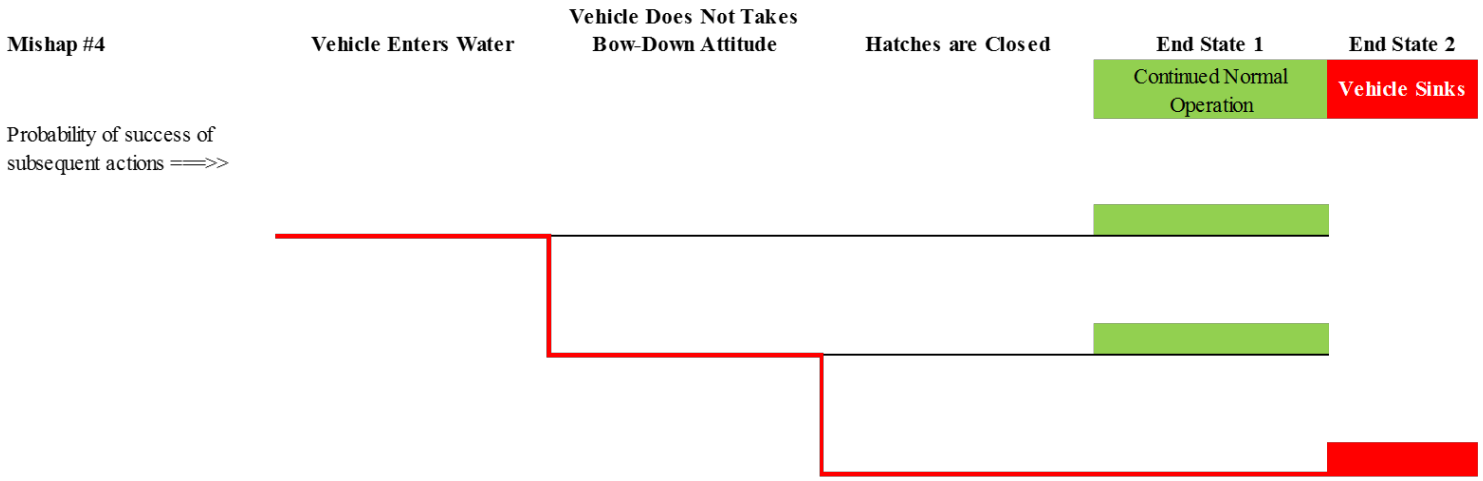

Figure 17. Mishap #4 Event Tree.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. MISHAP #2 CUT SET—SAPHIRE DATA

#	Cases	Prob/Freq	Total %	Cut Sets	
		1.233E-7	100	Displaying 16 Cut Sets. (16 Original)	
1	C	1.000E-7	81.07	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-1		GENERATOR_DISABLED_WATER	Water intrusion disables generator. NOTE: This should be updated with probability of water intrusion for missing bolts
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
2	C	1.000E-8	8.11	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-1		GENERATOR_DISABLED_WATER	Water intrusion disables generator. NOTE: This should be updated with probability of water intrusion for missing bolts
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader

#	Cases	Prob/Freq	Total %	Cut Sets	
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
3	C	1.000E-8	8.11	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-2		GENERATOR_DISABLED_OTHER	Other reasons for the generator being disabled
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
4	C	1.000E-9	0.81	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-2		GENERATOR_DISABLED_OTHER	Other reasons for the generator being disabled
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
5	C	1.000E-9	0.81	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-1		GENERATOR_DISABLED_WATER	Water intrusion disables generator. NOTE: This should

#	Cases	Prob/Freq	Total %	Cut Sets	
					be updated with probability of water intrusion for missing bolts
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
6	C	1.000E-9	0.81	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
		1.000E-3		VEHICLE_BATTERIES_OTHER	Other reason for vehicle batteries discharging
7	C	1.000E-10	0.08	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-1		GENERATOR_DISABLED_WATER	Water intrusion disables generator. NOTE: This should be updated with probability of water intrusion for missing bolts
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge

#	Cases	Prob/Freq	Total %	Cut Sets	
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
8	C	1.000E-10	0.08	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
		1.000E-3		VEHICLE_BATTERIES_OTHER	Other reason for vehicle batteries discharging
9	C	1.000E-10	0.08	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-2		GENERATOR_DISABLED_OTHER	Other reasons for the generator being disabled
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC

#	Cases	Prob/Freq	Total %	Cut Sets	
10	C	1.000E-11	< 0.01	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-2		ENGINE_RESTART_OTHER	Other reasons for engine not restarting successfully
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-3		LOSS_OF_ELEC_BILGE_OTHER	Other reasons for losing the electric bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
11	C	1.000E-11	< 0.01	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-2		GENERATOR_DISABLED_OTHER	Other reasons for the generator being disabled
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
12	C	1.000E-11	< 0.01	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge

#	Cases	Prob/Freq	Total %	Cut Sets	
		1.000E-3		LOSS_OF_ELEC_BILGE_OTHER	Other reasons for losing the electric bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
13	C	1.000E-11	< 0.01	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-2		OTHER_PLENUM_BOLT_FAILUR	Other reasons for plenum bolts failing or missing
		1.000E-1		PREOPS_UNSECURED_SL	During preops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During preops, unsecured plenum door not identified by the VC
		1.000E-3		VEHICLE_BATTERIES_OTHER	Other reason for vehicle batteries discharging
14	C	1.000E-12	< 0.01	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge
		1.000E-3		LOSS_OF_ELEC_BILGE_OTHER	Other reasons for losing the electric bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts

#	Cases	Prob/Freq	Total %	Cut Sets	
		1.000E-1		PREOPS_UNSECURED_SL	During pre-ops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During pre-ops, unsecured plenum door not identified by the VC
15	C	1.000E-12	< 0.01	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-3		HYDRAULIC_BILGE_OTHER	Other reasons for losing hydraulic bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-1		PREOPS_UNSECURED_SL	During pre-ops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During pre-ops, unsecured plenum door not identified by the VC
		1.000E-3		VEHICLE_BATTERIES_OTHER	Other reason for vehicle batteries discharging
16	C	1.000E-12	< 0.01	MISHAP_2: 4	
		1.000E+0		SPLASH	Vehicle enters the water (either from ship or shore)
		1.000E-3		COLLISION_W_RCVRY_ASST	Prior collision with a recovery asset to damage plenum bolts
		1.000E-2		ENGINE_RESTART_OTHER	Other reasons for engine not restarting successfully
		1.000E-1		ENGINE_STALL	Engine stalls
		1.000E-3		LOSS_OF_ELEC_BILGE_OTHER	Other reasons for losing the electric bilge
		1.000E-1		MAINT_MISSING_BOLT_UNIDE	Maintenance does not identify missing or damaged bolts
		1.000E-1		PREOPS_UNSECURED_SL	During pre-ops, unsecured plenum door not identified by the section leader
		1.000E-1		PREOPS_UNSECURED_VC	During pre-ops, unsecured plenum door not identified by the VC

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bourne, Brett A. 2009. *Command Investigation into the Circumstances Surrounding the Sinking of the Assault Amphibious Vehicle (AAVP7A1) Tactical Number S106, USMC Number 522450 that Occurred on 11 June 2010*. Official Memorandum. Camp Pendleton, CA: United States Marine Corps.

Commanding General Second Marine Division. 1994. *Endorsement of BLT Three Slant Two Report of Mishap File Number 94004*. Camp Lejeune, NC: United States Marine Corps.

Cowan, Shawn R. 2009. "A Human Systems Integration Perspective to Evaluating Naval Aviation Mishaps and Developing Intervention Strategies." Master's thesis, Naval Postgraduate School.

Department of Defense (DoD). 2012. *System Safety*. DoD MIL-STD-882E. Washington, DC: Department of Defense.

Department of the Navy (DoN). 2005. *Navy & Marine Corps Mishap and Safety Investigation, Reporting, and Record Keeping Manual*. OPNAVINST 5102.1D. Washington, DC: Department of the Navy.

———. 2012a. *Manual of the Judge Advocate General*. JAGINST 5800.7F. Washington, DC: Department of the Navy.

———. 2012b. *Preventive Maintenance Checks and Services, Lubrication Instructions and Operational Checklists for the Assault Amphibious Vehicle, Family of Vehicles.* Technical Instruction 09674A OD/1. Washington, DC: Department of the Navy.

Ericson, Clifton A. 2005. *Hazard Analysis Techniques for System Safety*. Hoboken, NJ: Wiley-Interscience.

Gibson, W. Huw, and Barry Kirwan. 2008. "Application of the CARA HRA tool to Air Traffic Management safety cases." *EEC* (May). www.researchgate.net/profile/Barry_Kirwan/publication/228973246_Application_of_the_CARA_HRA_tool_to_Air_Traffic_Management_safety_cases/links/00b49527a0fe901926000000/Application-of-the-CARA-HRA-tool-to-Air-Traffic-Management-safety-cases.pdf .

Islam, Rabiul, Faisal Khan, Rouzbeh Abbassi, and Vikram Garaniya. 2018. "Human Error Probability Assessment during Maintenance Activities of Marine Systems." *Safety and Health at Work* 9, no. 1: 42–52.

Jensen, John B. 1999. “Simulation and Analysis of Class A and B TACAIR Flight Mishaps with an Assessment of Human Factors Intervention.” Master’s thesis, Naval Postgraduate School.

Kirwan, B., H. Gibson, R. Kennedy, J. Edmunds, G. Cooksley, and I. Umbers. 2005. “Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool.” *Safety and Reliability* 25, no. 2: 38–45.

Nespoli, Claudio, and Sabatino Ditali. 2010. “Human Error Probability Estimation for Process Risk Assessment with Emphasis on Control Room Operations.” In *4th International Conference on Safety & Environment in Process Industry* (10). DOI: 10.3303/CET1019036.

Stamatelatos, Michael. 2011. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. 2nd ed. Washington, DC: NASA.

Seiffert, Brain F. 2011. *Board of Inquiry (BOI) into the Facts and Circumstances Surrounding the Sinking of t Amphibious Assault Vehicle (AAV) 522785 (S103) During Basic Water Driving Class for Students of the Basic Vehicle Repairman Course (BVRC 2-11) on 14 January 2011*. Official Memorandum. Camp Pendleton, CA: United States Marine Corps.

Strack, Brian L. 2010. *Command Investigation into the Circumstances Surrounding the Assault Amphibian Vehicle Mishap that Occurred on 20 April 2009*. Official Memorandum. Camp Lejeune, NC: United States Marine Corps.

United States Marine Corps (USMC). 2012. *Assault Amphibious Vehicle 7A1 Family of Vehicles.* Technical Manual 09674A-10/3D. Washington, DC: United States Marine Corps.

———. 2013. *Standard Operating Procedures for Assault Amphibious Vehicle Operations (COMMON SOP FOR AAV OPS)*. Battalion Order P3000.1I. Camp Pendleton, CA: United States Marine Corps.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California