Toward a Probabilistic Risk Assessment (PRA) Method for Assessing Mishaps in Legacy Systems Using Mishap Reports

Conference Paper *in* INCOSE International Symposium · July 2020

DOI: 10.1002/j.2334-5837.2020.00772.x

CITATIONS
0

READS
162

4 authors, including:

Bryan O'Halloran
Naval Postgraduate School
64 PUBLICATIONS **476** CITATIONS

SEE PROFILE

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **937** CITATIONS

SEE PROFILE

30th Annual INCOSE international symposium
Virtual Event
July 20 - 22, 2020

Toward a Probabilistic Risk Assessment (PRA) Method for Assessing Mishaps in Legacy Systems Using Mishap Reports

Joseph Dean
PEO Land Systems
Quantico, VA 22134
joseph.dean1@usmc.mil

Bryan M. O'Halloran
Naval Postgraduate School
Monterey, CA
bmohallo@nps.edu

Douglas L. Van Bossuyt
Naval Postgraduate School
Monterey, CA
Douglas.vanbossuty@nps.edu

Rachel Mourning
Centauri
Lexington Park, MD 20653
Rachel.Mouring@centauricorp.com

Abstract. There is a significant delta between the acknowledged probability of potential mishaps under the current safety assessment approach derived from Military Standard 882E (MIL-STD-882E), Department of Defense Standard Practice of System Safety, and what is observed from actualized mishaps being reported. When assessing systems safety during the design process, the approaches used that comply with MIL-STD-882E simplify the mishap scenario by assuming a single initiating mechanism. By decomposing mishap reports from legacy systems, fault and event trees are used to identify common failure modes that were not adequately assessed under the current process. Each of the mishap reports assessed has identified more than one initiating mechanism. As such, this work suggests a greater mishap probability than was originally acknowledged. To address the current limitation, this work develops (1) an approach for decomposing mishap scenarios for legacy systems to identify mishaps resulting from multiple failure modes, (2) a method for systematically implementing the mishap decomposition on the assessed system or newly designed systems, and (3) a list of characteristics for an improved systems safety method.

Introduction

The United States Department of Defense (DoD) utilizes more complex systems than any other entity in the world. Their need for the effective utilization of system is a critical concern to their operation. System safety represents an important contributor to their operation, and therefore the continued desire for its improvement.

The risks formally associated with the system are often articulated and acknowledged differently from the risks realized during its operation. MIL-STD-882E (DoD 2012) is the standard methodology utilized for the identification, assessment, and mitigation of risks associated with the development, test, production, use, and disposal. This standard focuses on single-failure events and does not generally include failure modes that require sequential failure events to occur, and therefore the application of MIL-STD-882E during design works well for identifying and mitigating catastrophic single-point failures. The direct causal 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 AVs 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). The "1E" level of risk is a *catastrophic* severity and an *improbable* probability of occurrence. Relative to the predicted 1E risk, the associated occurrence of AAV mishaps have demonstrated that reassessment of the mishaps is necessary. 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 work 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. This is accomplished by assessing detailed mishap reports. The decomposition of the AAV mishaps included in this work do not divulge specific information on individual incidents, but rather are used to identify generalized trends and causes that are useful to this research. Given the complexity of mishap reports that contain high-severity mishaps, this research develops a systematic approach to deriving the specific information that is needed to construct an accurate understanding of the mishap. The output is also constructed in a way that is desirable for being used as an input to MIL-STD-882E. Further, the output of this work is being used to inform the development of a risk-based method that is better suited for assessing system safety risk during design. As such, this work concludes by suggesting attributes that would exist in a risk-based method for assessing systems safety.

Background and Related Work

A wide variety of methods have been embraced for assessing systems safety (Leveson 2011, Hollnagel 2012). The current safety assessment state of practice for military systems is largely influenced by MIL-STD-882E (DoD 2012). There are several analyses referenced within this standard, with examples including system hazard analysis (SHA), subsystem hazard analysis (SSHA), and operating and support hazard analysis (O&SHA), that are intended to identify, assess, and mitigate hazards associated with the manufacturing, transportation, storage, and operation of the system. While these methods are well-intentioned, the majority of their application and approach is left to interpretation. This limitation leads to significant variation on how they are applied. Further, the comprehensive application of this military standard, especially through the use of the Hazard Tracking System (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. As such, an approach that allows multiple hazards in relation to a mishap is necessary.

The Failure Reporting, Analysis, and Corrective Action (FRACA) methodology is commonly used to identify the cause and mitigation for observed failures (Series 2009). FRACA is implemented in a variety of ways depending on the system and organization. A common element of the method is to identify the failure's root cause(s); classical approaches to this step include (1) "the five whys," (2) a fault tree, and (3) and Ishikawa (or Fishbone) diagram. The first approach is informal and not useful for rigorous assessment. Ishikawa diagrams have the benefit of segregating the root cause into specified groups, allowing the practitioner to focus on identifying potential root causes that are related to the group. Extensions to the Ishikawa diagram have focused on case studies demonstrating its use for determining the root cause of a failure (Ilie 2012, Gawdzińska 2011). Given these extensions, the Ishikawa diagram omits logic and therefore are not suitable for being used within probabilistic methods such as PRA. Further, while FRACA is generically used for identifying and fixing failures, the method does not associate the failure's root cause with the full set of the system's effect; instead, it relates one observed system effect relating to its full set of potential root causes. The limitation reduces its application in designing a system.

PRA has been used in the development of certain products or procedures such as nuclear power plants, aircraft, spacecraft, and automobiles/passenger vehicles (Gibson and Kirwan 2008). 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 (HRA) has also grown to better understand how humans relate to mishap scenarios. Specific HRA techniques have been developed to further quantify and increase the accuracy of specific PRA models (Nespoli and Sabatino 2010). Islam et al. leveraged existing HRA techniques such as the 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 (Islam et al. 2018). While these methods have application to mishaps and the integration of humans in a mishap scenario, they are not useful for comprehensively understanding historical mishaps.

Mishap analysis research is often centered on the human component of the system. For example, Jensen assesses flight mishaps for while considering human factors (Jensen 1999). Similarly, Cowan develops intervention strategies for naval aviation mishaps using concepts from human systems integration (Cowan 2009). While both analyze mishap reports and focus their evaluation on the human casual factors, their work is focused on aviation related systems and mishaps. Further, their work emphasizes the human element of the mishap. For most systems using in the military, including the AAV used as a case study in our work, emphasizing one element of the system can lead to overlooking other elements. The goal of the mishap decomposition presenting in this research is to identify the facts of the mishap regardless of the nature.

While many methods exist in the literature that may be useful in specific situations, a holistic method applicable to analyzing mishaps for military systems does not currently exist. Of the methods that do exist, the primary focus is on aspects of human reliability. As a result, this research focuses on the decomposition and assessment of mishap scenarios to understand the causal relationships and sequences of events and to allow for scenarios where multiple failure modes are present.

Specific 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). 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 during the time of the initial safety assessment. 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, practitioners will be better informed of the current risks of their systems as designed and operated. While this research focuses on legacy system, this approach is analogous when applied for identifying high-risk events during the development of new system; this perspective would depend on analogous system and would be most effective when the newly designed system shares a significant relationships to the legacy system. Either perspective offers the practitioner to an approach to become aware of the risks and take actions to improve the safety.

A Decomposition Approach for Mishap Scenarios in Legacy Systems

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. Due to these limitations, a goal of this research is to analyze real-world AAV mishaps to identify conditions, factors, root causes, and trends that lead to the mishaps with the goal to develop a risk-based method that is better suited for the complex systems, especially amphibious vehicles such as the AAV. To achieve this outcome, a deep understanding is required for assessing mishap reports. This section discusses the AAV operations, historical mishaps, and develops an approach for decomposing the mishap events based on the available reports. The findings show that all of the AAV mishaps investigated as part of this research are the result of a chain of events that cannot be traced back to a single casual factor.

AAV Operations

An understanding of AAV operations is necessary to comprehend the sequence of events that comprise mishap reports; the following operations descriptions focus on embarking and debarking where the majority of high severity mishaps have historically occurred. 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 nominally 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 AAV surfaces and is transitioned to the objective ashore (USMC 2012).

Mishap Description

The following are brief descriptions of the mishap scenario used in this paper. This mishap scenario has been developed using the mishap investigation report. The formal mishap investigative report provides a detailed fact-based chronological history of the vehicle and crew. The reports generated are the result of extensive investigation and contain a significant amount of information. The analysis of the reports allows the identification of the contributing conditions and associated causal factors.

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 contacted 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.

A Reverse Engineering Approach to Mishap Decomposition

Each of the mishaps investigated in this research were 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.

In preparation for decomposing the mishap report, a coding of information is used to understand the important aspect of the process. The elements of the coding approach are used to identify specific information with the mishap report. The mishap reports used in this research have been developed in accordance with Judge Advocate General Instruction 5800.7F (DoN 2012a), section 0209.d. The details in the mishap investigation report are communicated in two forms; findings of facts and opinions. The information within these two categories comprises the coding approach. 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). In contrast, the opinions (O) are reasonable evaluations, inferences, or conclusions of the investigating officer based on the findings. This coding approach is used in this research to extract relevant information from each mishap report, which allows the analyst to identify the key elements among the findings and opinions that contributed to the mishap. The coding approach itself is intentionally basic; the complexity of the mishap and its report promotes the need for a simple coding approach.

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 both the vehicle and its 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, based on the vehicle's original safety assessment.

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 investigating during this research, utilizing the approach described here, are not presented due to limited space. Instead, one example is provided.

1. 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.

Methodology

This section presents a methodology that is applicable to legacy systems to identify the set of failure modes that have caused a mishap. Its development is based on findings derived from the mishap decomposition previously presented. The method, presented in Figure 1, is used to identify the types of failure modes that have been presented previously in the Mishap Description section. These failure modes may have occurred previously on the legacy system or on related system. Further, the method is also used to model the relationships between the identified failure modes. The results can be compared to the original safety analysis (e.g., MIL-STD-882E for an AAV) to characterize the gaps in assessment of the mishaps.

The Mishap Assessment method in Figure 1 is comprised of three independent steps. In summary these steps include (1) data collection, (2) building mishap scenario models, and (3) identifying failure modes. To illustrate the application of the proposed method to the AAV, the use of the previously described mishap will be used.

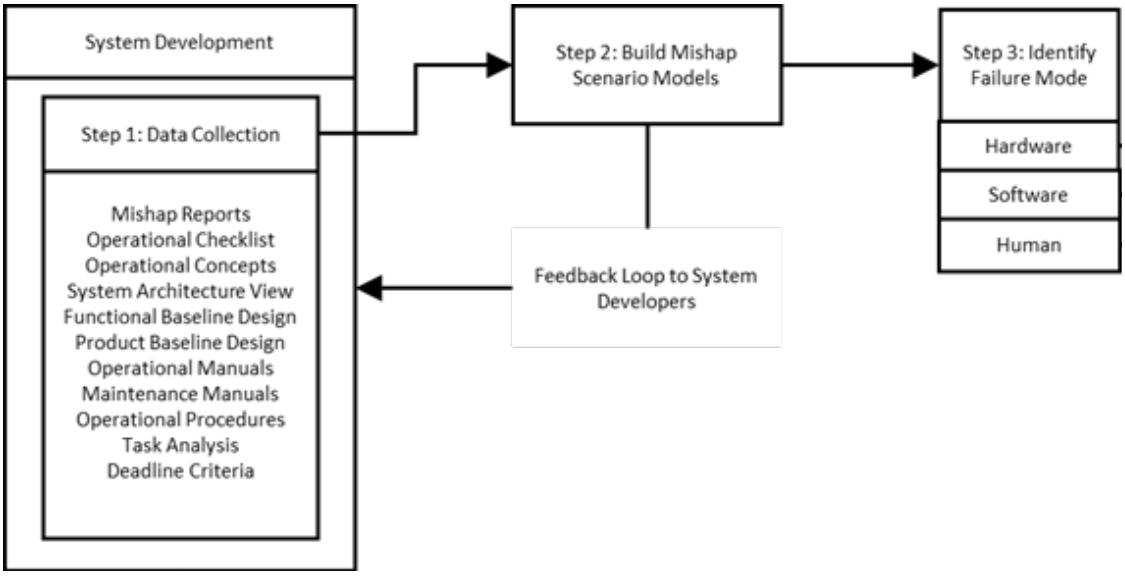

Figure 1. Mishap Assessment Method.

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 and completeness of the

documentation collected. Mishap reports, operational checklists, operational tasks, and procedures need to be collected. 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 identify failure modes, thus the primary data collection focuses on the mishap report and pre-water operations checklists.

Step 2: Mishap Scenario Models

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

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.

It is 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. Each of these have substantially different means for determining the probability of failure. Computing or sourcing the related probabilities is not addressed in this research. Figures 3 and 4 show and fault tree and the event tree for the mishap scenario.

Research Findings

This section presents discussion and insight into the mishap decomposition and method previously presented. The majority of the mishaps assess have been omitted from this paper due to space. However, the discussion and insight presented within this section has also been derived from the mishaps that are not presented.

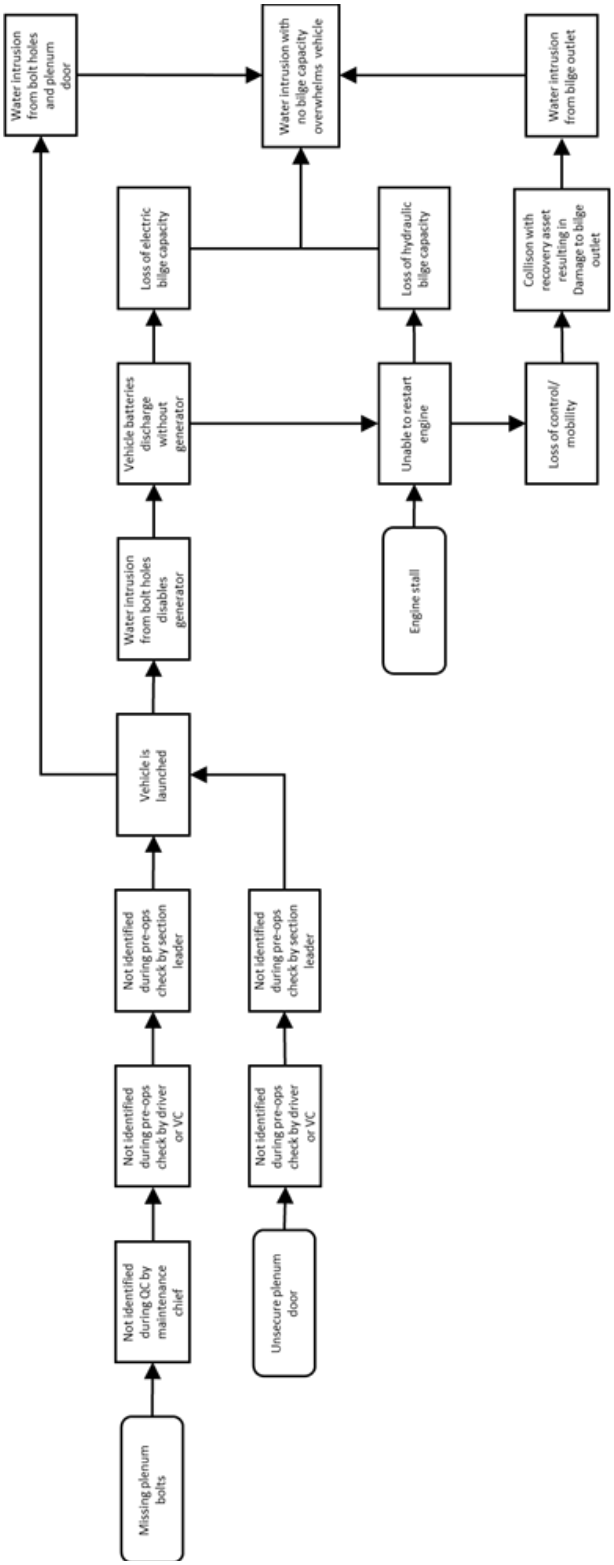

Figure 2. Mishap Scenario Model

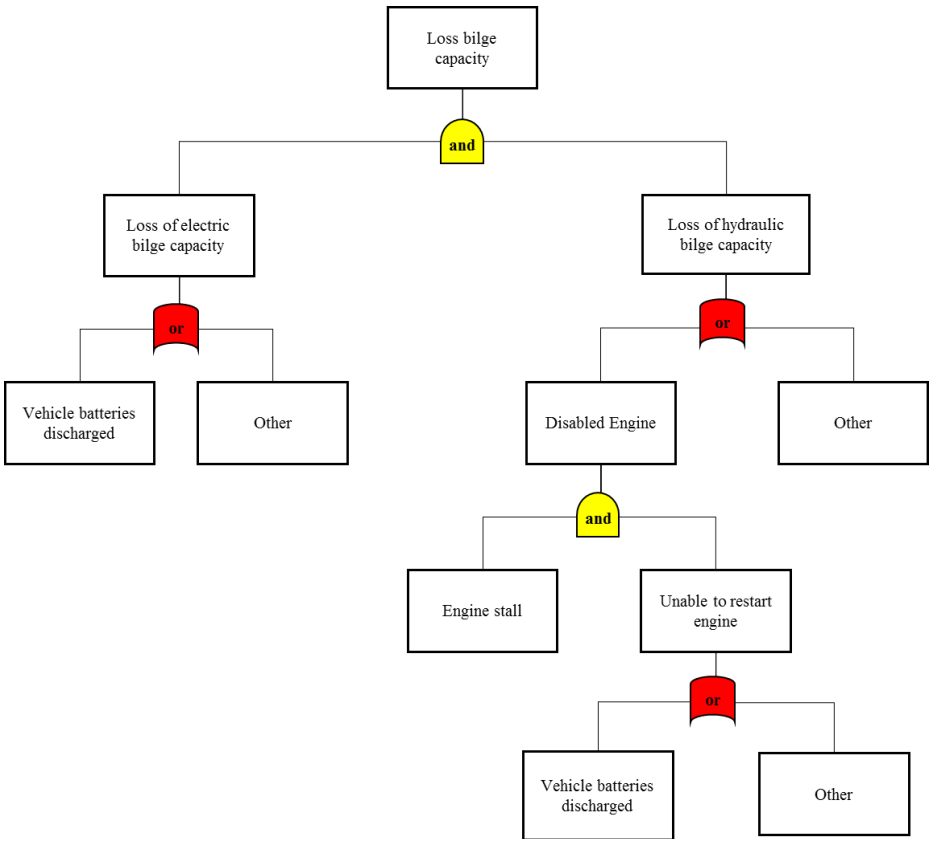

Figure 3. Loss of Bilge Capacity FTA

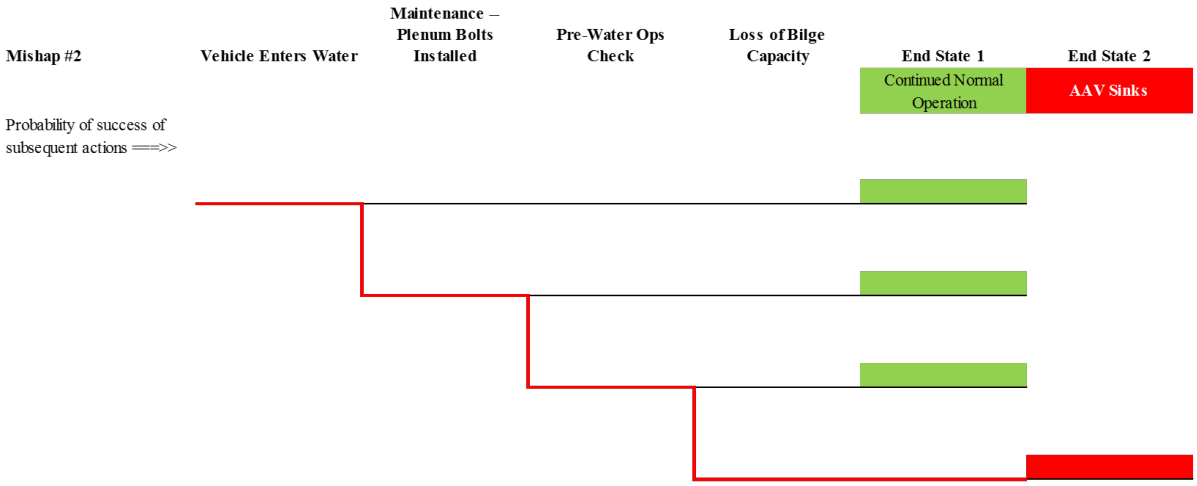

Figure 4. Mishap Scenario Event Tree

Understanding the Results of Multiple Mishap Decompositions

The mishap decomposition process has been repeated for several mishaps scenarios. The majority of examined mishaps resulted in the same end state: the vehicle submerges/sinks. This finding is strongly related to assessing the highest severity mishaps. There are several similar failure events

that are also common across the mishaps. These failure events often shared the same casual factor origins. Two examples include (1) poor quality control during maintenance operations, and (2) failure to conduct pre-operations check/pre-water operations check. The reoccurrence of casual factor origins presents strong evidence for changes to the system or its operation.

Each of the mishaps assessed share a common human related casual factor, human error, or violation, and are underrepresented by applying existing safety methods in MIL-STD-882E. 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; however, the 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.

Redefining Systems Safety Terms

Based on the findings of this work, several systems safety related definitions are proposed which are inclusive of multiple causal events. The intent of adjusting the existing definitions is to create a better alignment the mishap scenarios that occur. To understand the changes in each definition relative to those found in MIL-STD-882E, the original MIL-STD-882E definitions are shown here (DoD 2012):

- 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, and to better align definitions with the mishap scenarios that occur during a system’s operation, the following definitions are proposed:

- Mishap: A sequence of event(s) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
- Hazard: A set of one or more conditions that lead to the event.
- Causal factor: An initiating event that contributes toward triggering one or more hazard(s).

Desired Attributes of a Risk-Based Method for Systems Safety

This section suggests potential improvements to MIL-STD-882E methods based on the research conducted. This is approached by highlighting core elements that exist in current MIL-STD-882E methods as well as those that would exist within an improved risk-based method. While the following suggestions are proposed based on this assessment of the AAV mishap scenarios, the intent of MIL-STD-882E is to comprehensively cover a variety of system types.

An improved safety assessment method shall be a comprehensive analysis method focused on identifying and assessing 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, or in some cases a related system. Table 1 illustrates the correlation between the desired characteristics and the current methodologies in MIL-STD-882E to highlight the gap.

Table 1. Attributes of an improved risk-based method for systems safety

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

Discussion and Future Work

While the method is developed for legacy systems, the method can 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.

While the development of a method applied retroactively may appear to have limited value, especially since the mishaps have occurred and traditional analysis is performed during the design of the system, it serves two specific uses. First, due to the substantial cost of modern systems, lifecycle extensions are becoming more common. Lifecycle extensions are used to verify a system beyond its original lifetime. The method in Figure 1 is an ideal approach to better understanding

the safety of the system if it is to be extended. The second use of this method is to be used for analogous systems. Systems are rarely developed in a way that they are uniquely new. A newly designed system has heritage in prior systems. For the use of this method on newly developed systems, they should be similar in system type and operation; for example, the design of a new generation of AAVs.

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 method should be applied across the full operational profile of the system. Further, the results identified within this research will be presented relative to the results found using MIL-STD-882E. This will offer a clear perspective into the gap between the current standard and the possible future state of the standard.

Conclusion

The risks associated with the equipment provided to the warfighter are often articulated and acknowledged quite differently from the risks realized during operation. 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. 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, as indicated with the AAV example.

Real world mishaps occur regularly in system, but the occurrence of high severity mishaps is relatively low. And while existing methods identify many of the potential mishaps during design, the work presented in this paper is used to critically assess the remainder. Specifically, this work is used to identify failure causes that lead to their occurrence, especially where multiple failure causes are allowable. The development of a safety-based method that (1) employs fault and event trees and (2) is specific to the operational scenarios of the system and the decomposed mishap reports allowed the observed risk to be assessed. The proposed method demonstrates that there is a potentially significant difference between the acknowledged mishaps and those assessed in the mishaps reported. This research has identified this result to be 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.

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.
Gawdzińska, K., 2011. Application of the Pareto chart and Ishikawa diagram for the Identification of Major Defects in Metal Composite Castings. ISSN (1897-3310), 11(2).
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.
Hollnagel, E., 2012. FRAM, the functional resonance analysis method: modelling complex socio-technical systems. Ashgate Publishing, Ltd.
Ilie, G. and Ciocoiu, C.N., 2010. Application of fishbone diagram to determine the risk of an event with multiple causes. Management research and practice, 2(1), pp.1-20.
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.
Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. MIT press.
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.

Series, A.E., Standard: Performance-Based Failure Reporting, Analysis & Corrective Action System (FRACAS) Requirements (ANSI/AIAA S-102.1. 4-2009).

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.