Accurate Risk Assessment Using Multi-Relational Hazard/Mishap Pairings

Regina A. Eller, BA; Department of the Navy, Naval Surface Warfare Center,
Dahlgren Division; Dahlgren, Virginia, USA

Michael G. Zemore, MS Sys Eng; Department of the Navy, Naval Surface Warfare Center,
Dahlgren Division; Dahlgren, Virginia, USA

Rani A. Kady, Ph.D.; Department of the Navy, Naval Surface Warfare Center,
Dahlgren Division; Dahlgren, Virginia, USA

Keywords: risk assessment, multiple effects, hazard tracking

Abstract

Current methods for defining safety risk force a single "worst case" assessment. Unfortunately, the worst case assessment approach fails to capture the complexity of hazard/mishap relationships or the reality of multiple effects from any given mishap. This failure limits a complex risk picture to be characterized using only a portion of the relevant safety engineering and assessment data. This paper describes focused research to suggest an innovative methodology for defining risk associated with multiple hazard contributors and multiple effects. Research focus areas included defining complex hazard path relationships, mathematical calculations of risk, and the development of requirements for a relational engineering tool. The combined research and results is intended to transform Military Standard (MIL-STD)-882E, *Department of Defense Standard Practice for System Safety*, (ref. 1) based mishap risk assessment from a worst case into a complex, multi-contributor, risk definition and accurately characterize risk using combined effects of personnel injury, equipment/property damage, and environmental damage.

Introduction

The Naval Surface Warfare Center, Dahlgren Division (NSWCDD), houses the largest concentration of system safety engineers for the Navy. From Marine Corps infantry weapons to major naval combat systems, Dahlgren safety engineers must continue to be innovative in an era of increasingly complex warfare and systems. To ensure system safety engineering maintains track with the development, research devoted to advancing safety methodology needs to be conducted. This will continue to ensure the highest degree of safety possible for the people who use weapon systems in the conduct of their duties. The Naval Innovative Science and Engineering (NISE) Program has allowed NSWCDD to conduct focused research in the area of system safety. The NISE Program was established by the Duncan Hunter National Defense Authorization Act for Fiscal Year (FY) 2009 (ref. 2). The goal of NISE is to ensure that the vitality of Naval Warfare Centers' in-house laboratories is maintained by supporting the development of beneficial, innovative, high-risk Research, Development, Testing, and Evaluation (RDT&E) solutions/technologies.

NISE funding was granted to NSWCDD for a proposal titled "Accurate Risk Assessment Using Multi-Relational Hazard/Mishap Pairings." The results of the research include a methodology and a set of requirements for a tool that will support the safety engineer to fully characterize and track mishap risk. The methodology transforms the existing approach of single hazard and effect risk based on worst case characterization, into an integrated assessment considering all possible hazards, hazard causal factors, mishaps, and effects. This advancement will allow the safety engineer and risk managers to make more informed decisions and focus on key risk factors and contributors that may have been concealed using previous assessment and tracking approaches. This paper will summarize the results of the research completed under the NISE Program.

Definitions

Baseline/Version: An agreed-to description of the attributes of a product, at a point in time, which serves as a basis for defining change.

Causal Factor: A failure, condition, or event that contributes either directly or indirectly to the existence of a hazard. One or several mechanisms that can trigger a real or potential hazardous condition.

Effect: A result or consequence brought about by some cause. Defined in terms of harm to personnel, equipment/property, and the environment.

Event: An occurrence, especially one that is particularly significant. Examples include structural test firing, operational test, or operational deployment.

Hazard: A real or potential condition that can lead to an unplanned event or series of events (i.e., mishap) resulting in personnel injury, damage to or loss of equipment/property, or damage to the environment.

Mishap: An unplanned event or series of events resulting in unintentional death, injury, occupational illness; damage to or loss of equipment or property; or damage to the environment.

Mishap Group: Group of associated mishaps that communicate risk areas and an aggregate assessment of like mishaps for presentation to the signature authority.

Phase: A distinct stage of development. A defined period of time within the life cycle of a system. Examples of phases include the following: production, transportation, installation operation, test and evaluation, and disposal.

Relationship: Establishing a connection between trouble reports, causal factors, hazards, mishaps, or mishap groups.

Trouble Report (TR): A mechanism used to track the detection, reporting, and resolution of a realized problem identified during development, testing, use of the system. This realized problem can potentially contribute either directly or indirectly to the existence of a causal factor or hazard.

Problem Statement

MIL-STD-882 serves as the overarching document that guides safety programs for the Department of Defense (DoD). MIL-STD-882 details the analytical tasks that should be performed when conducting a comprehensive safety program. On 11 May 2012, MIL-STD-882E was released that modified the approach for system safety away from worst case risk assessments to most credible risk assessments that capture multiple effects of a mishap. Safety historically focused on high severity/low probability risks, but this modification to MIL-STD-882E also encourages assessment and mitigation of high probability/low severity risks.

Developing a methodology to assess multiple effects and hazard paths immediately brings in several problem areas that need to be characterized and resolved. The methodology needed to address the following considerations:

1. Identifying the relationships between safety objects that serve as the basis for risk assessment. Clearly define the risk assessment required for each relationship established for TRs, causal factors, hazards, mishaps, and the concept of mishap groups.
2. Defining a process for risk assessment of the multiple effects (personnel injury, equipment/property damage, and environmental damage) without over inflation of risk. Ensure process remains in line with the risk assessment policy outlined in MIL-STD-882E and the Naval Sea Systems Command Instruction (NAVSEAINST) 5100.12B, *System Safety Engineering Policy* (ref. 3).
3. Avert taxing safety engineer with performing multiple replications of hazard data. A multi-relational tool must support the safety engineer's ability to perform risk assessments without duplication.
4. Supports the volume and complexity of a multitude of system safety programs from element, combat systems, and platform. Allow for growth in the area of force level and integration and interoperability.

Hazard Relationships

To advance the practice of identifying hazard relationships to fully characterize risk, we must first understand the current method in place. In Figure 1, it can be seen that the causal factor relates to a single hazard, and the hazard

relates to a single mishap. Risk assessment, whether for the causal factor or the hazard, focuses on the potential mishap and its worst or most credible outcome to determine the risk for each causal factor and hazard. For example, each causal factor is assessed for its potential to cause or contribute to that mishap and the worst or most credible effect, and assigned a risk of high, serious, medium, or low, accordingly. Even though there is a relationship to the hazard, the risk assessment focuses on the causal factors contribution to mishap potential. Similarly, each hazard is assessed for its potential to cause or contribute to the mishap and the worst or most credible effect, and is assigned a severity of mishap and likelihood that mishap will occur.

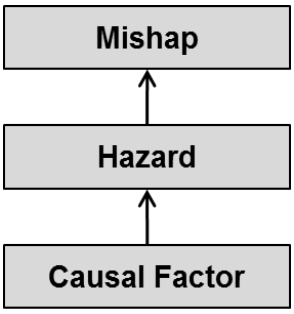

Figure 1 — Worst Case / One- to-One Relation

That structure, although sensible and systematic, leaves many risks unassessed and undocumented. Figure 2, illustrates the true complexity of the relationships. It can be seen that the TRs can relate to multiple causal factors and hazards, a single causal factor can relate to multiple hazards, a hazard can relate to multiple mishaps, and mishaps can aggregate into mishap groups. This identification of all possible relationships, without duplication, allows the safety engineer to consider all associated hazard paths. In other words, if several causal factors relate to a hazard and it is determined the hazard is more likely to cause a mishap as a result; the risk assessment for the hazard should reflect that increased probability of mishap. If the engineer realizes a single hazard is influencing the risk of multiple mishaps, that advancement will provide the risk managers a significant tool allowing more fully informed decisions and focus on key risk factors and contributors that may have been concealed using previous assessment and tracking approaches.

Within the relationship structure identified in Figure 2, there is a separation of TRs to be separate objects in the hazard path than the causal factor. According to definition, a TR is a mechanism used to track the detection, reporting, and resolution of a realized problem identified during development, testing, and use of the system. TRs are generally generated by an organization outside of system safety, but still need to be analyzed by the safety community to identify potential contribution to safety risk. While a causal factor is a failure, condition, or event that contributes either directly or indirectly to the existence of a hazard, causal factors are an artifact of hazard analysis and not a single reporting of a failure or system event. Tracking TRs separate from causal factors allows the safety engineer to communicate to the test community, configuration control boards, and the system engineering team to the safety risk of that individual failure. Assessing TRs allows safety to influence plans for correction and build priorities. Distinguishing TRs as a separate object in the hazard path supports the safety engineer to have the ability to appropriately status each object. A software TR identified during testing of the system may be coded, tested, and verified prior to deployment of the system that would indicate the appropriate status of “Closed” within the hazard tracking database. But the causal factor may continue to be a valid hazard path that needs to be communicated in the assessment of safety risk.

The term mishap group was developed during the course of the NISE research to aid in the risk assessment process defined in NAVSEAINST 5100.12B. A mishap group is defined as an aggregate assessment of like mishaps. Mishap groups will be used in support of risk acceptance and the generation of Mishap Assessment Reports (MARs). MARs are the vehicle to inform the appropriate signature authority and gain risk acceptance according to risk level. The term mishap group will replace the term of top-level mishap which is currently in use by many safety programs at NSWCDD. Top-level mishap tends to generate confusion that the particular mishap under discussion represents the highest severity and most probable risk assessment. Mishap group is designed to alleviate confusion with the term top-level mishap. The concept of mishap group is not required to be implemented within the methodology discussed in this paper.

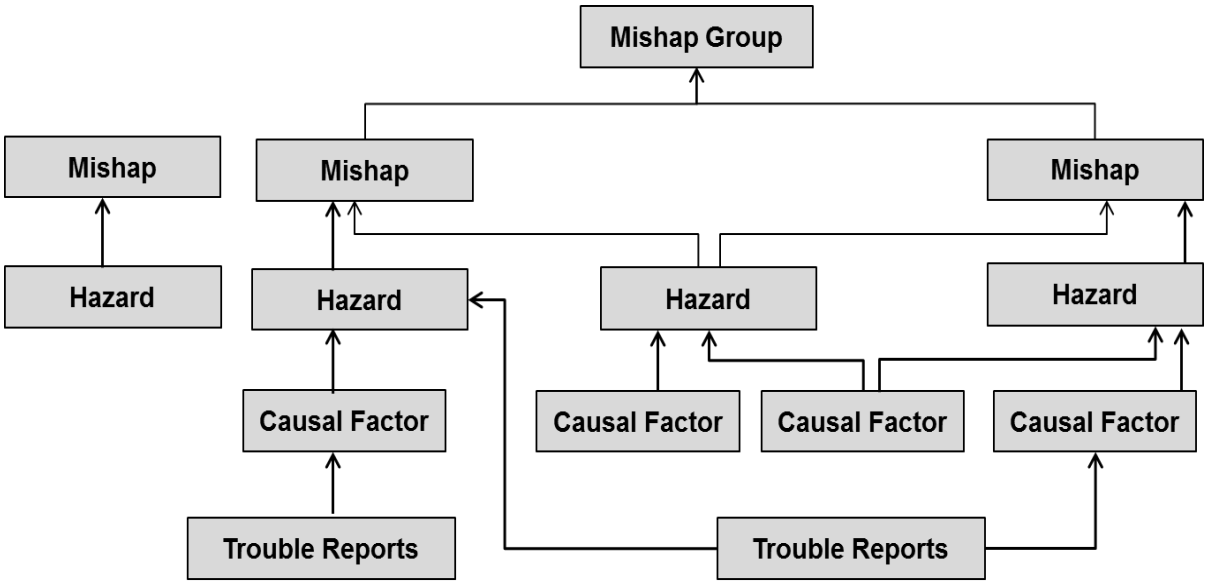

Figure 2 — Multiple Hazard Paths / Many- to-Many Relationship

Risk Assessment

With acknowledgment of all possible relationships between TRs, causal factors, hazards, mishaps, and mishap groups it is possible to begin defining a methodology for risk assessment. This methodology complies and builds on the guidance provided in MIL-STD-882E. Risk assessment is the activity of 1) examining each identified causal factor to refine the description of the risk, identifying and verifying mitigations, determining the effects, and assigning risk level (high, serious, medium or low); or 2) examining each identified hazard to refine the description of the risk, identifying and verifying mitigations, determining the effects, and assigning a Risk Assessment Code (RAC). Risk assessment is influenced by the causal factor(s)/hazard relationship(s), the event, the phase, potential mishap, potential effects of the mishap, and applicable baseline/version. Based on all those factors and any change in those factors, it may be necessary to re-assess the risk. A single object may require multiple risk assessments and acceptances throughout its life cycle.

Each object in the hazard path, as illustrated in Figure 2, requires a risk assessment. The following details the influences to define risk for each object and the required assessments. The process outlined allows for and illustrates the standard method and the advanced method developed during research. It is realized that all hazard paths are not multi-relational. When the hazard path is not multi-relational, it is not necessary to execute the advanced methodology. The advanced methodology allows the engineer to fully examine all possible hazard paths when required. The following details the factors in assessing risk for each object:

- Mishap Group
  - Risk assessment is the worst case mishap value for each effect (personnel injury, equipment/property damage, and environmental damage) of all related mishaps per the risk ranking values.
- Mishap
  - The aggregate assessment of more than one related hazard, or if only one related hazard, the mishap assumes the risk of the hazard.
- Hazard
  - The potential impact the individual hazard, with associated causal factors, could have on personnel, equipment/property, and the environment documented as probability and severity for each of the three effects (i.e., personnel, equipment/property, and environment) in relation to the potential mishap.
- Causal Factor

    - The risk associated with the existing system and its potential to cause a mishap as a mechanism that triggers a hazard, or the risk associated with the potential for mishap as a result of the unimplemented change request as documented in the causal factor.
- Trouble Report
    - The risk associated with the existing system and its potential to cause a mishap as a mechanism that triggers a causal factor or hazard, or the risk associated with the potential for mishap as a result of the unimplemented change request as documented in the TR.

Communication of risk factors is crucial to effectively influencing programmatic decisions to eliminate hazards or mitigate those hazards when elimination is not possible. Development of a standard format to communicate and define safety risk drivers will aid in an effective safety program. Table 1 details for each object in the hazard path the risk drivers that need to be considered, the risk format, the risk assessments, and how the risk should be reported to decision makers.

- Risk drivers are identified as relationship, baseline/version, event, and phase. During the risk assessment phase or when additional information is received, if any additional risk drivers are identified the safety engineer should investigate for a potential change in the risk assessment. If the risk driver indicates that the risk has changed it should be fully documented.
- In accordance with DoD policy, the risk format for each object is defined. For mishap groups, mishaps, and hazards the standard is to assess risk in the format of a RAC or Mishap Risk Index (MRI). For example, a 1C RAC is defined as high risk level where the first number (e.g., 1) represents severity and the second character (e.g., C) represents probability. For TRs and causal factors the risk format utilized is detailed in MIL-STD-882E (Table B-1) using a ranking of high, serious, medium, or low.
- Risk assessment for each object includes initial risk level (assessment of risk prior to investigation and development of mitigation strategy), current risk level (assessment at the present time factoring in all relevant data), and target risk level (assessment expect to achieve by implementing specific recommended mitigations). For mishap group, mishap, and hazards there are two approaches. Utilizing the standard method a single RAC for each effect will be assigned. Using the advanced method, a RAC is assigned for each severity in relationship to the effect.
- Risk reporting provides instruction on summarizing risk assessments at all levels to aid in proper communication of risk. The methodology supports NAVSEAINST 5100.12B at the mishap group, mishap, and hazard level. The risk ranking methodology provides a tool for the safety engineer to determine the worst case assessment. Figure 3 provides the numerical value for each box in the MIL-STD-882E RAC matrix which is used to evaluate an automatic worst case assessment. If the ranking is the same for the worst case risk for multiple effects, the effect of personnel injury shall take precedence over equipment/property damage, and equipment/property damage shall take precedence over environmental damage as the overall risk assessment.

Table 1 — Risk Assessment Process

Object	Risk Drivers	Risk Format	Risk Assessment	Risk Reporting
Mishap Group	Relationship Baseline/ Version Event Phase	Risk Assessment Code	<u>Standard Method</u> Single RAC for each Effect Personnel Injury (Initial, Current, Target) Equipment/Property Damage (Initial, Current, Target) Environment Damage (Initial, Current, Target)	Single RAC for Mishap Group
			<u>Advanced Method</u> RAC for each Severity Personnel Injury (Initial, Current, Target) Equipment/Property Damage (Initial, Current, Target) Environment Damage (Initial, Current, Target)	RAC for each Mishap Group Effect (Worst Case Assessment using Risk Ranking)

Object	Risk Drivers	Risk Format	Risk Assessment	Risk Reporting
Mishap	Relationship Baseline/ Version Event Phase	Risk Assessment Code	Standard Method Single RAC for each Effect Personnel Injury (Initial, Current, Target) Equipment/Property Damage (Initial, Current, Target) Environment Damage (Initial, Current, Target)	Single RAC for Mishap
			Advanced Method RAC for each Severity Personnel Injury (Initial, Current, Target) Equipment/Property Damage (Initial, Current, Target) Environment Damage (Initial, Current, Target)	RAC for each Mishap Effect (Worst Case Assessment using Risk Ranking)
Hazard	Relationship Baseline/ Version Event Phase	Risk Assessment Code	Standard Method Single RAC for each Effect Personnel Injury (Initial, Current, Target) Equipment/Property Damage (Initial, Current, Target) Environment Damage (Initial, Current, Target)	Single RAC for Hazard
			Advanced Method RAC for each Severity Personnel Injury (Initial, Current, Target) Equipment/Property Damage (Initial, Current, Target) Environment Damage (Initial, Current, Target)	RAC for each Hazard Effect (Worst Case Assessment using Risk Ranking)
Causal Factor	Baseline/ Version Event Phase	High, Serious, Medium, Low	Initial Risk Level Current Risk Level Target Risk Level	Single Risk Level
Trouble Report	Baseline/ Version Event Phase	High, Serious, Medium, Low	Initial Risk Level Current Risk Level Target Risk Level	Single Risk Level

Figure 3 — MIL-STD-882E Risk Assessment Matrix with Risk Ranking Values

RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	1	3	6	10
Probable (B)	2	5	9	14
Occasional (C)	4	8	13	18
Remote (D)	7	12	16	19
Improbable (E)	11	15	17	20
Eliminated (F)	21			

Mathematical Computation of Risk

Research in the area of mathematically assessing aggregate risk is an ongoing safety effort. Numerous papers have been published and are being worked to discover an approved and validated method in which to aggregate risk assessments. In conjunction with the NISE research on risk assessment, NSWCDD partnered with the Office of Naval Research to have a summer professor of mathematics focus on aggregating risk. Dr. Arjuna Ranasinghe from Alabama A&M University, Applied Mathematics, conducted focused research in this area. The question posed was if each hazard has a probability it could lead to mishap, is it possible to define the probability the mishap and associated effects could occur based on all contributing hazards? The results of the research are documented in a paper titled "*Multi-Relational Risk Assessment Model (MRRAM) for Personnel Injury, Equipment, and Environment Damages due to Missile Launch with a given set of Hazards*." At this time research has not provided a method for calculation of risk that is mature enough to embed within the framework of the relational tool.

Development of Requirements

During the NISE research project two main goals were developed. The first goal was to develop the methodology for accurately defining risk associated with multiple hazard contributors and multiple effects. The second goal was to develop a detailed set of requirements for a database that would support the advanced risk assessment methodology. The requirements detail a web-based, relational, closed-looped database used to enter, maintain, capture, and report mishap risk for safety hazards, causal factors, and the collection thereof. The tool will support the safety engineer in transforming the existing approach of a single hazard and effect risk based on worst case characterization, into an integrated assessment considering all possible hazards, hazard causes, mishaps, and effects.

The requirements define a database specifically focused on safety. The database will be available for use across all safety programs at NSWCDD from elements, combat systems, and platforms. Developing a detailed set of requirements that capture the risk assessment process for NSWCDD allows the process to become repeatable and consistent among the 100+ customers that NSWCDD serves. The requirements are divided into the following sections:

- System Requirements - This section describes the "non-functional" requirements that define the quality of the system at a high level. Examples of some of these high level requirements include: security, maintenance, relational features, web-based, permission hierarchy allowing approved cross program access, and advanced reporting capabilities.
- Functional Requirements - The requirements in this section describe the core functionality of what the system is to accomplish, including descriptions of the functions that the tool will need to carry out. Each functional step, from importing data, assessing risk, tracking hazards, and reporting risk, is detailed in the requirements.
- Data Requirements - This section provides the definitions and describes the data relationships and attributes to be held within the database. Key attributes include data to be stored, amount of data, field size, field definition, and retention characteristics (period and archival requirements).

Conclusion

NISE funding has allowed focused research into advancing the methodology in conducting safety risk assessments. Research focused on three interconnected goals for investigation; 1) advancing risk assessment methodology, 2) investigating mathematical solutions to aggregating multi-relational effects, and 3) developing database requirements for a tool to implement the developed methodology. Benefits from advancement in safety risk assessment techniques will reduce the mishap risk the warfighter will experience. System safety will be able to accurately communicate a complete set of risk drivers that is inclusive of all possible effects and will result in providing decision authorities with accurate and cost effective mitigation strategies. The ability to identify significant risk factors, as those that influence multiple mishap scenarios, enhances the ability to focus on the most influential risk factors to gain substantially more safety risk mitigation.

References

1. MIL-STD-882E, *Department of Defense Standard Practice System Safety*, 11 May 2012.

2. Public Law 110-417, *Duncan Hunter National Defense Authorization Act for Fiscal Year 2009*.

3. NAVSEAINST 5100.12B, *System Safety Engineering Policy*, 3 August 2011.

Biography

Regina A. Eller, Safety Analyst, Naval Surface Warfare Center, Dahlgren Division, 5375 Marple Road, Suite 153, Dahlgren, VA 22448-5155, USA, telephone – (540) 284-1115, facsimile – (540) 653-3125, email – regina.eller@navy.mil.

Regina A. Eller is currently a safety analyst for the Naval Surface Warfare Center, Dahlgren Division. She holds a Bachelor of Arts from the University of Mary Washington. She has nine years of safety experience supporting both Combat Systems and Element Safety Programs. Current assignment is supporting the Ship Self Defense System (SSDS) MK 2 safety program which is the key element of the combat system deployed on multiple Navy platforms.

Michael G. Zemore, Chief Engineer, Naval Surface Warfare Center, Dahlgren Division, 5375 Marple Road, Suite 151, Dahlgren, VA 22448-5155, USA, telephone – (540) 653-7881, email – michael.zemore@navy.mil.

Michael G. Zemore is Chief Engineer to the Systems Safety Engineering Division of the Naval Surface Warfare Center, Dahlgren Division. He holds a Bachelor of Science degree in Electronics Engineering Technology from DeVry Institute of Technology and a Master of Science Degree in Systems Engineering from Virginia Polytechnic Institute and State University. He has 28 years of experience in system safety engineering as it applies to surface Navy combat systems, integrated shipboard training systems, radar systems, fire control systems, launching systems, missile systems, force protection, and nuclear weapon systems. He has authored numerous articles and conference papers on system safety topics.

R. A. Kady, System Safety Engineer, Naval Surface Warfare Center, Dahlgren Division, 5375 Marple Road, Suite 153, Dahlgren, VA 22448-5155, USA, telephone – (540) 653-2409, email – rani.kady@navy.mil.

Dr. Kady is a system safety engineer in the Combat Systems Safety Branch. He provides system safety support to unmanned ground vehicle programs. He received his Ph.D. in Industrial and Systems Engineering with an emphasis in safety from Auburn University. His research interests include risk analysis, software safety, and system safety training.

NSWCDD-PN-14-00412 is approved for Distribution Statement A:
Approved for Public Release; distribution is unlimited.