The Challenges of a Quantitative Approach to Risk Assessment

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

Arjuna Ranasinghe, Ph.D.; Alabama A&M University, Mathematics Department;
Huntsville, Alabama, USA

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

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

Keywords: mishap probability, risk assessment, quantitative analysis, risk documentation

Abstract

Risk assessment and documentation, as an element of the system safety process in the general requirements of Military Standard (MIL-STD)-882E, *Department of Defense Standard Practice System Safety*, assesses the severity category and probability level of a potential mishap. The likelihood of occurrence of a mishap determines the probability level for a given hazard at a given point in time. Since quantitative assessments are perceived to be more accurate than qualitative ones, several attempts have been made to accurately measure the appropriate probability level for a hazard. Researchers of such attempts are challenged to use appropriate and representative data to define frequency or rate of occurrence for a hazard. This paper describes the nature and complexity of a mathematical representation to risk assessment. A Multi-Relational Risk Assessment Model (MRRAM) is presented to outline a detailed quantitative risk assessment approach and guide the system safety community attempts. A case study is also presented to illustrate the application of MRRAM to quantify risk assessment and highlight the challenges to the system safety community in terms of mathematical approach, assumptions, and variable conditions of risk assessment.

Introduction

Element 3 of the system safety process in the general requirements of MIL-STD-882E (ref. 1) is assess and document risk. According to MIL-STD-882E, risk is defined as "combination of the severity of the mishap and the probability that the mishap will occur." Therefore, risk is expressed by severity category and probability level of the potential mishap(s) for each hazard across all system modes. A hazard is a real or potential condition that could lead to (a) mishap(s), and is triggered by one or several causal factors. Such relationship between causal factor, hazard, and mishap is depicted in Figure 1. The relationship is rarely simple and direct. A mishap is often the result of several hazards which are triggered by several mechanisms (causal factors). A true representation of such relationship, due to the complexity of current systems, often requires many-to-many relationships between causal factors, hazards, and mishaps, as illustrated in Figure 2.

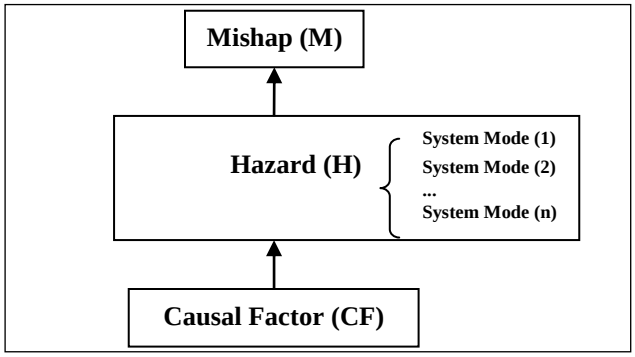


Figure 1 — Simple One-to-One Causal Factor-Hazard-Mishap Relationship

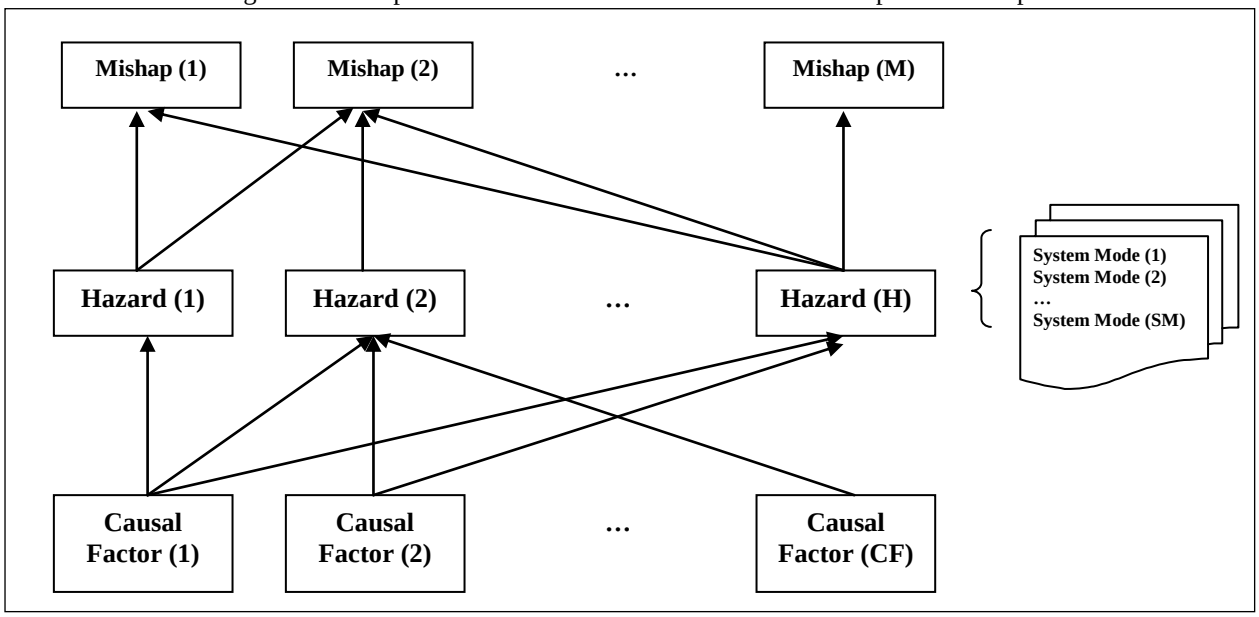


Figure 2 — Many-to-Many Causal Factors-Hazards-Mishaps Relationships

Quantitative Risk Assessment

MIL-STD-882A (ref. 2) required the introduction of hazard probability and established categories for frequency of occurrence. In MIL-STD-882B (ref. 3), risk was expressed as "the possibility of a mishap in terms of hazard severity and hazard probability." It characterized a hazard in terms of hazard severity categories and hazard probability levels. The term "Hazard Probability" referred to "the aggregate probability of occurrence of the individual hazardous events that create a specific hazard." In other words, hazard probability is the summation of hazardous event probabilities. MIL-STD-882C (ref. 4) dropped hazardous event and hazard event probability terms as components of hazard and hazard probability, respectively. Although it did not change the characterization of risk in terms of hazard severity and hazard probability, MIL-STD-882C focused on the "impact of mishap" instead of "mishap" alone.

MIL-STD-882D (ref. 5) introduced a new perspective to risk assessment. The term "Assessment of Mishap Risk" referred to "the severity and probability assessment of the mishap risk associated with each identified hazard." This is the first time risk is characterized in terms of mishap severity and mishap probability. Therefore, "Mishap Probability" referred to "the aggregate probability of occurrence of the individual events/hazards that might create a specific mishap." Such occurrence was presented in arbitrary categorizations (levels).

Although MIL-STD-882E (ref. 1) uses the term Risk Assessment Code (RAC) to express risk assessment (the severity category and probability level of the potential mishap(s) for each hazard across all system modes), the representation of risk in terms of severity and probability has been emphasized in previous versions of MIL-STD-882. A risk level of High, Serious, Medium, or Low is assigned for each RAC. In order to determine the appropriate probability level for a given hazard at a given point in time, the likelihood of mishap occurrence (probability) is calculated. Accurate and representative quantitative data that defines frequency or rate of occurrence of the mishap for a given hazard is preferable. The frequency is the actual or expected number of mishaps during a specified exposure. Figure 3 summarizes the evolution of quantitative risk assessment in MIL-STD-882.

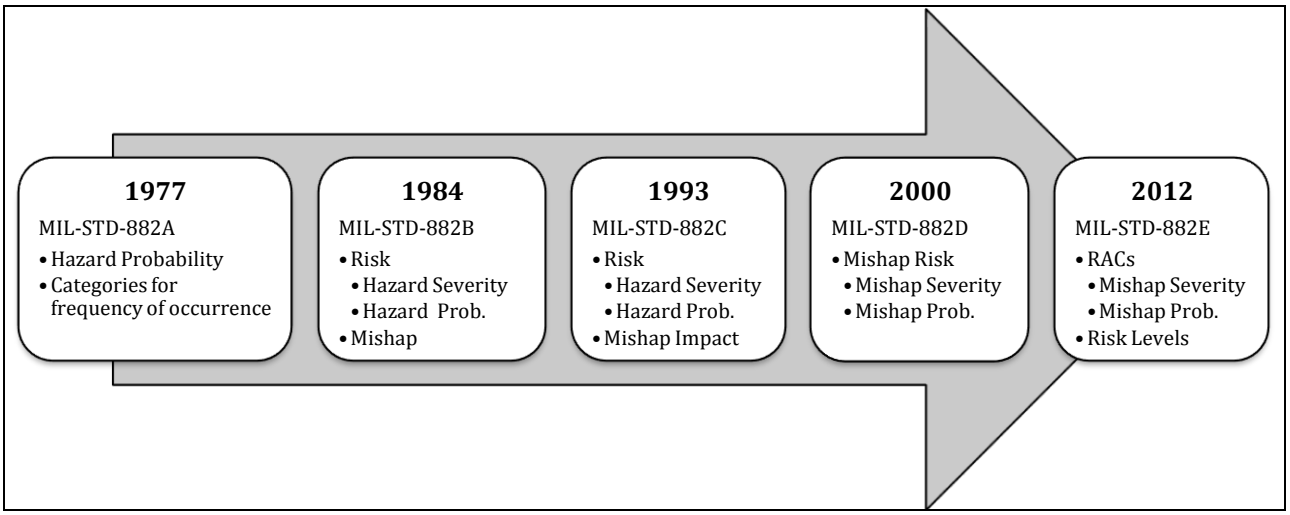


Figure 3 — The Development of Risk Assessment in MIL-STD-882

Background

Several attempts in system safety literature have been made to address quantitative risk assessment. One attempt (ref. 6) proposed a method to estimate the one hazard risk index (probability level and hazard severity) that best represents the cumulative risk of all the hazards in a Hazard Risk Assessment Matrix (HRAM). The proposed method tried to address the question "is the cumulative risk associated with lower risk hazards, each of which can be accepted by a lower level of authority, equal to a risk that should be accepted by a higher level of authority?" The answer to the question depends on the subjectivity of assigning Hazard Risk Index (HRI) to a hazard since the probability levels and the hazard categories are described qualitatively. Another study (ref. 7) developed a methodology to address uncertainty with respect to aircraft crashes (mishaps). The method utilized a frequency distribution function to calculate confidence intervals for the frequency (probability) of a crash (mishap). The probability of the mishap is a combination of several random variables and constants. Monte Carlo techniques were used to generate a histogram for the probability of the mishap.

Cooper (ref. 8) demonstrated how the numeric inputs and outputs of probabilistic analyses can be enhanced by new mathematical approaches to convey much more information than a single fixed number or even a probabilistic spread of numbers representing variability or uncertainty. Taubel (ref. 9) developed a multiple severity method to determine mishap risk by plotting the probability of a mishap with respect to all of the possible mishap severities, in terms of monetary units, using multiple point estimates or a cumulative distribution function. The results can be used to determine the acceptable cost for mitigating the risk and compare the life cycle cost of the risk before and after mitigation.

Finally, Banerjee (ref. 10) proposed a Composite Risk Index (CRI) based on probability and severity that takes into account the human perception of equivalent risk. The study questioned Naval Sea Systems Command Instruction (NAVSEAINST) 5100.12B (ref. 11) logarithmic risk chart with respect to probability. The study mathematically derived and expressed probability of any hazard in terms of any other in order to compare between different probability levels. The study used perception to express severity. Given the acceptance authority changes between "High and Serious" and "Medium and Low," a line can be defined at the threshold between Medium and Serious that transgresses all four severity levels. As a result, the study concluded that risk is perceived equal at severity-probability combinations of 1E, 2D, 3C, and 4A.

The previous attempts to quantify risk assessment with respect to severity and probability did not address the relationship between causal factors, hazards, mishaps, and effects as described in MIL-STD-882E (ref. 1). The studies isolated probability and/or severity to quantify risk assessment. This paper is not a new attempt to quantify risk assessment but rather guidance to system safety practitioners of how to mathematically approach risk assessment given a path forward to assess risk for a safety program based on a multi-relational risk assessment.

The Multi-Relational Risk Assessment Model

MRRAM was the result of a summer research partnership between the Naval Surface Warfare Center, Dahlgren Division (NSWCDD), Office of Naval Research (ONR), and Alabama A&M University. MRRAM attempts to mathematically represent the complex relationship between hazards, mishaps, and effects. It follows the MIL-STD-882E approach to define such relationship. MRRAM guides system safety practitioners to quantify risk utilizing multiple contributing factors and multiple potential effects in order to assign a complete yet comprehensive risk assessment in terms of RACs. The Model assumes a finite number of independent but not mutually exclusive hazards that lead to a mishap or a set of mishaps. MRRAM also defines the probability of a mishap based on contributing hazards. The effects of a mishap are defined in terms of personnel injury, equipment damage/loss, and environment damage. MRRAM combines the probability of a mishap with the probability of an effect. The collective aggregate probability considers a combination of personnel injury, equipment damage/loss, and environment damage in order to eliminate the hazard or reduce the associated risk. Figure 4 illustrates the MRRAM framework. Although, the Model does not quantify causal factor(s) that would trigger the hazard(s), Figure 4 demonstrates the relationship between causal factor(s) and hazard(s), as well.

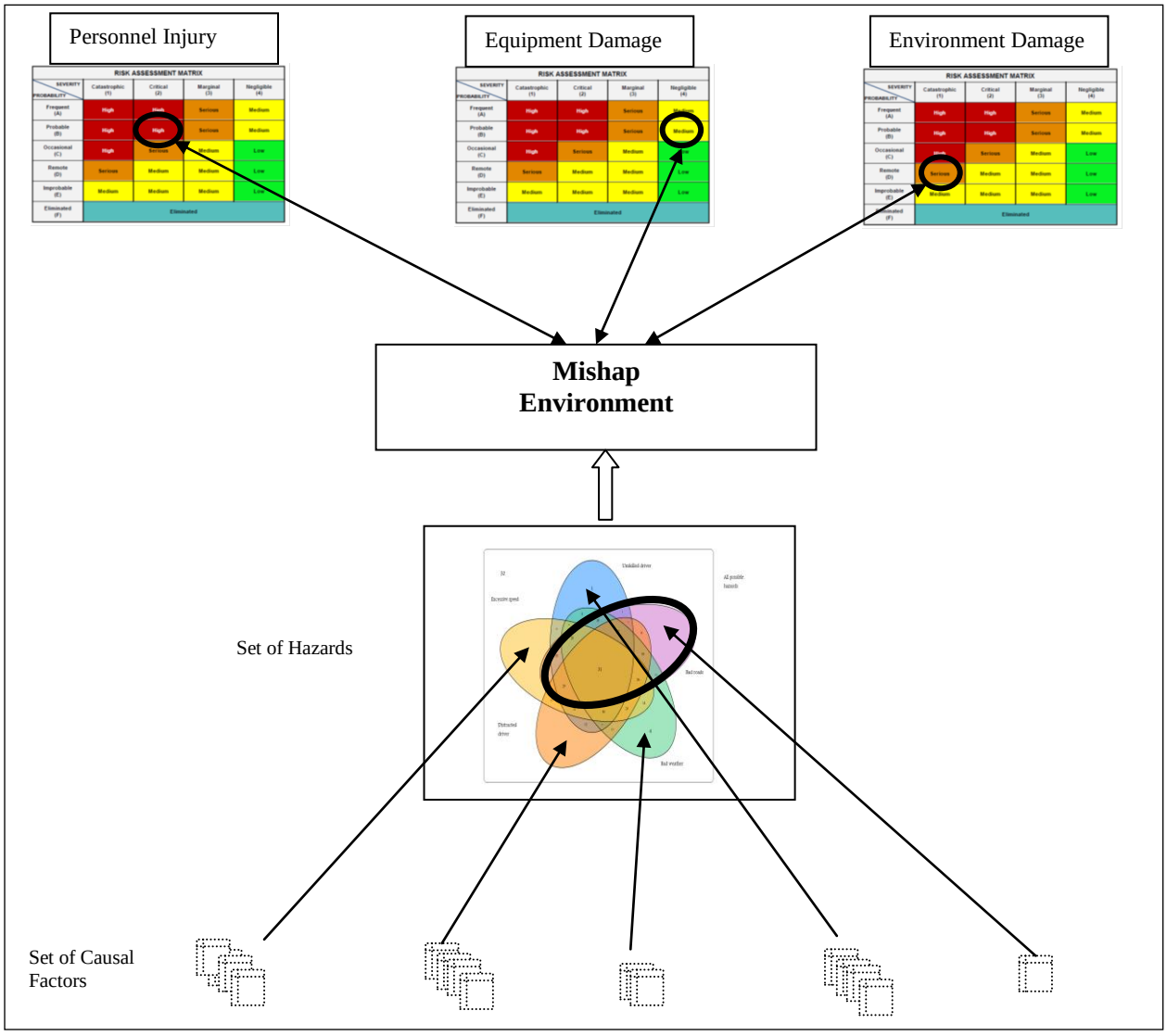


Figure 4 — MRRAM Framework

Once a set of independent and not mutually exclusive hazards for a mishap is defined, the total number of hazard combinations is calculated. The combination contains all possible ways of hazard grouping that would lead to a mishap. Figure 5 demonstrates the 32 combinations of 5 independent, not mutually exclusive, hazards namely A, B, C, D, and E. Since the hazards for a mishap contribute differently and often unequally, it is useful to capture the probability level of the potential mishap for a set of hazard combinations instead of individual hazards. For example, hazard A in Figure 5 includes the following hazard combinations 5, 6, 7, 10, 15, 16, 17, 18, 20, 21, 25, 26, 27, 28, 29, and 31. The MRRAM considers a set of hazard combinations to express a mishap probability level (Frequent, Probable, Occasional, Remote, and Improbable).

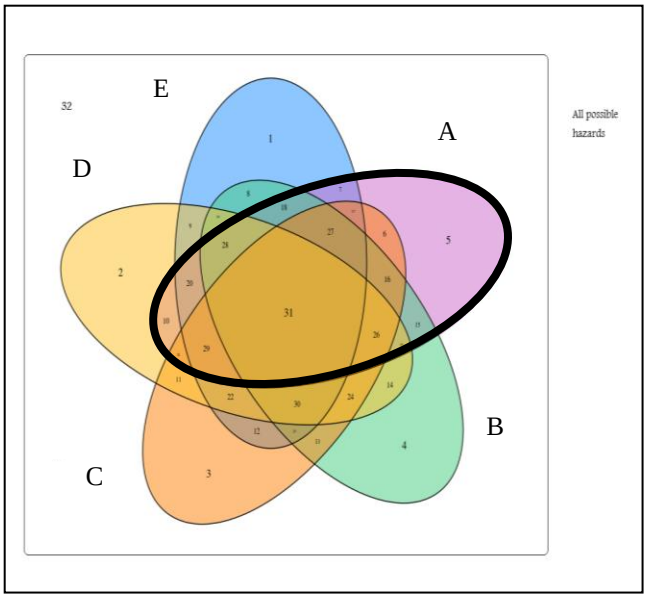


Figure 5 — Total Possible Combinations of 5 Hazards (A to E)

In addition to the mishap probability, the RAC captures the severity of a mishap for personnel injury, equipment damage/loss, and environment damage. Mathematically speaking, each severity has a chance to fall under one of the four severity categories of MIL-STD-882E; namely Catastrophic, Critical, Marginal, and Negligible. This results in 12 possible outcomes from severity and effect combinations. Table 1 lists the severity levels for each effect as adopted in MRRAM.

Table 1 — Severity Categories for Personnel Injury, Equipment Damage, and Environment Damage

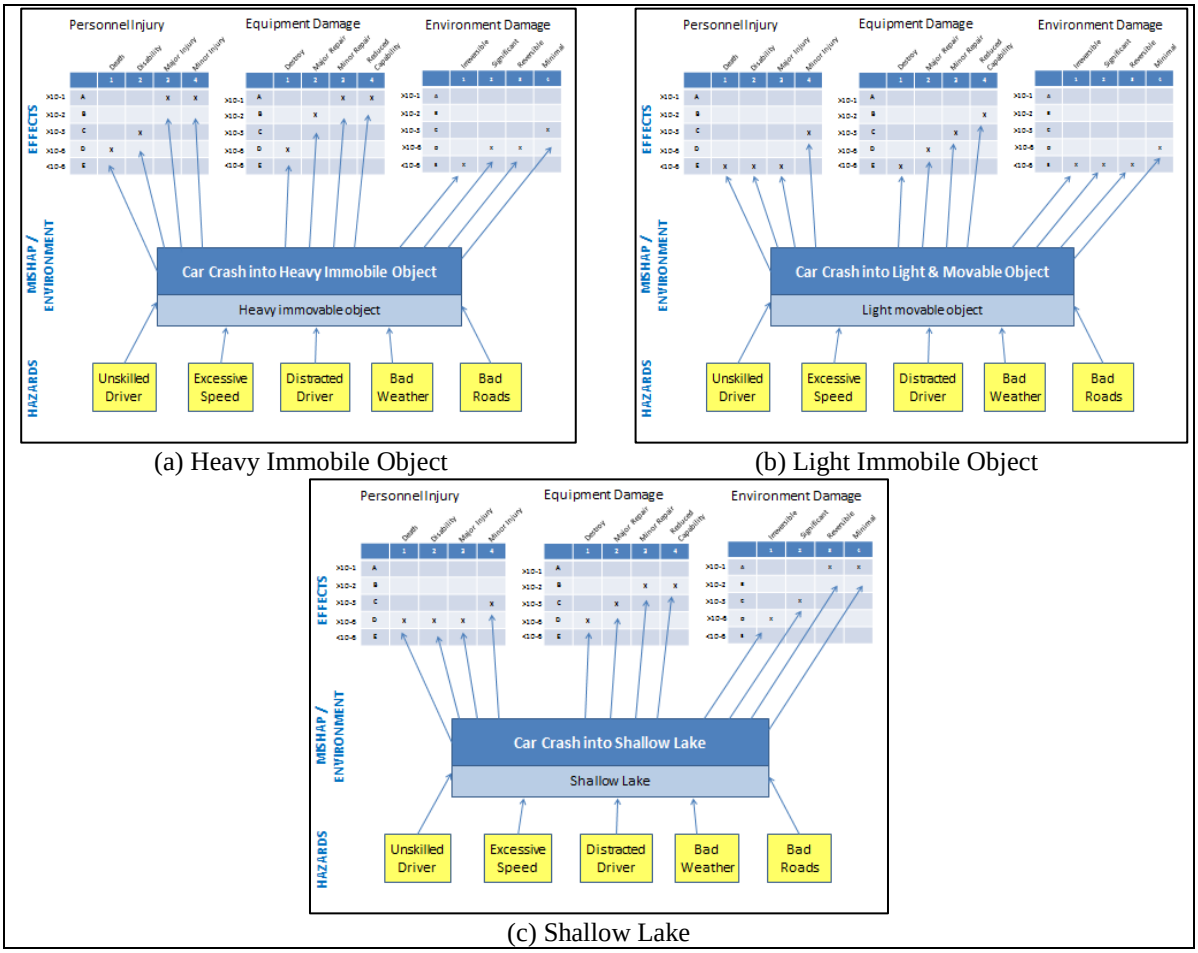
Description	**Severity Categories**	**Mishap Result Criteria**		
		Personnel Injury	**Equipment Damage/Loss**	**Environment Damage**
Catastrophic	1	Death	Destruction	Irreversible
Critical	2	Disability	Major Repair	Significant
Marginal	3	Major Injury	Minor Repair	Reversible
Negligible	4	Minor Injury	Reduced Capability	Minimal

MRRAM also accounts for the "environment" where the mishap takes place. This is a more accurate representation of a mishap. As the environment is defined, the likelihood of mishap occurrence within an environment is usually described. The summation of the likelihoods of mishap occurrence in different environments should be equal to the overall likelihood of mishap occurrence in general. Typical events such as developmental or operational testing, demonstrations, and fielding should help the system safety practitioner define the environment where the mishap is likely to occur.

Multi-Relational Risk Assessment Model Case Study

Due to the complexity of the mathematical representation of MRRAM, the following case study demonstrates the Model approach to quantify the relationship between hazards, mishaps, and effects based on MIL-STD-882E. It also highlights the level of data needed to accurately quantify risk assessment.

A car crashes into a heavy immobile object, a light and movable object, or near a lake. The crash is caused by an unskilled driver, excessive speed, distracted driver, bad weather, and/or bad roads. Any or a combination of these hazards could result in the car crash. The crash could result in personnel injury in terms of death, disability, major injury, or minor injury; equipment damage/loss in terms of destruction, major repair, minor repair, or reduced capability; and environment damage in terms of irreversible, significant, reversible, or minimal environmental damage. Figure 6 summarizes the mishap, hazards, environments, and effects of the car crash based on the "environment" of the car crash (mishap). The car crash case study includes five hazards (represented in yellow boxes in Figure 6). MRRAM does not represent the mathematical relation between hazards and causal factors. The level of representation starts at the hazards. The middle large box represents the mishap and environmental probability of the mishap. In other words, the probability the car crashes into a heavy immobile object, light mobile object, or a shallow lake (a, b, or c, respectively). The lines up point to the probability assessments of each severity outcome for each effect category.



(a) Heavy Immobile Object

(b) Light Immobile Object

(c) Shallow Lake

Figure 6 — MRRAM Representation of Mishap, Hazards, and Effects in 3 Environments a, b, and c

The objective of MRRAM is to mathematically illustrate how to assess risk through a combination of the severity of the mishap and the probability that the mishap will occur.

1. Mishap Probability.

The car crash probability lies between A (Frequent) and E (Improbable) mishap probability levels of MIL-STD-882E. Probability level F (Eliminated) is used when a hazard is eliminated.

2. Mishap Severity.
   The car crash severity lies between 1 (Catastrophic) and 4 (Negligible) mishap severity categories of MIL-STD-882E.

3. Mishap Result Criteria.
   Given the severity of the mishap (car crash), the mishap result criterion varies by the effect; namely personnel injury, equipment damage/loss, or environment damage. A total of 12 possible outcomes from severity and effect combinations are counted based on 4 severity categories and 3 categorical effects. As a result, the total number of possible (random) events for the car crash mishap is

$$\text{Number of random events} = 4 \text{ mishap severity categories} \times 3 \text{ categorical effects} \times 3 \text{ different environments} \times 5 \text{ mishap probability levels} = 180 \quad (1)$$

For example, an unskilled driver (hazard) crashing a car into a shallow lake (environment) causing a major injury (mishap result criterion) to personnel (effect) is a single event for the mishap. Calculating a mishap probability, if possible, which contributes to assessing the risk (expressed as RAC) within the context of this single event (for example) is the accurate approach and the intent of MIL-STD-882E.

Furthermore, since the mishap result criteria in MIL-STD-882E do not distinguish between personnel injury, equipment damage/loss, and environment damage, MRRAM calculates the aggregate multi-relational mishap probability for personnel injury, equipment damage/loss, and environment damage due to a car crash in a given "environment."

Conclusion

Risk assessment via the severity category and probability level of a potential mishap is an important element of the system safety process. Attempts have been made to quantify the probability or severity without an accurate mathematical representation of both. This study demonstrates the complexity of a mathematical representation of risk assessment given the multi-relational nature of causal factors, hazards, mishaps, and effects. The following are the challenges that face the system safety community when attempting to quantify risk assessment.

1. Safety programs rarely capture data to obtain the probability estimate of a mishap for a hazard.
2. Appropriate and representative quantitative data hardly exist.
3. The complex nature of the multi-relation of causal factors, hazards, mishaps, and effects leads system safety practitioners towards a qualitative risk assessment analysis approach.
4. Quantitative risk assessments are no more valid than their assumptions. More emphasis is needed to study and understand the underlying assumptions of existing quantitative risk assessment attempts before implementing in safety programs to assess risk.
5. System safety practitioners should consider "return on investment" to their programs before delving into risk assessment quantification.

References

1. MIL-STD-882E, *Standard Practice System Safety, Revision E*, 2012.

2. MIL-STD-882A, *System Safety Program Requirements, Revision A*, 1977.

3. MIL-STD-882B, *System Safety Program Requirements, Revision B*, 1984.

4. MIL-STD-882C, *System Safety Program Requirements, Revision C*, 1993.

5. MIL-STD-882D, *Standard Practices for System Safety, Revision D*, 2000.

6. Andrews, Sidney B. "Cumulative Risk in Hazard Risk Matrices." *Proceedings of the 22nd International System Safety Conference*, Providence, RI, August 2004, 2-6.

7. Alexander, Albert J., Clark, Randy M., Miller, Charles L., Rigdon, Douglas L. "A Probabilistic Aircraft Crash Methodology." *Proceedings of the 14th International System Safety Conference*, Albuquerque, NM, August 1996, 12-17.

8. Cooper, Arlin J. "The Application of New Mathematical Approaches to Probabilistic Safety Analysis." *Proceedings of the 15th International System Safety Conference*, Washington, D.C., August 2004, 13-17.

9. Taubel, Jason A. "Use of the Multiple Severity Method to Determine Mishap Costs and Life Cycle Cost Savings." *Proceedings of the 29th International System Safety Conference*, Las Vegas, NV, August 2011, 8-12.

10. Banerjee, Aaron " Equivalence of Risk: A Mathematical Approach" *Proceedings of the 29th International System Safety Conference*, Las Vegas, NV, August 2011, 8-12.

11. United States Department of The Navy, NAVSEAINST 5100.12B, System Safety Engineering Policy, Washington DC, Government Printing Office, 2011.

Biography

R. A. Kady, System Safety Engineer, 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 System 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.

A. I. Ranasinghe, Professor of Mathematics, Department of Physics, Chemistry, and Mathematics, 4900 Meridian Street, Huntsville, AL 35762, USA, telephone - (256) 372-4839, email - arjuna.ranasinghe@aamu.edu.

Dr. Ranasinghe received his Ph.D. degree in Applied Mathematics with Mechanical Engineering minor from the University of Alabama in Huntsville in 1991. He received his M.S. Degree in Mathematics minored in Computer Science from North Carolina Central University, and his B.S. Degree in Mathematics from University of Peradeniya, Sri Lanka. He is presently serving as a Professor of Mathematics at Alabama A&M University. During the past 10 years he has published over 20 refereed journal articles in scientific journals. His current research interests are: Partial Differential Equations, Fluid Dynamics, Large Deviation, Stochastic Control Theory, Statistical Analysis, and Pattern Recognition.

M. G. Zemore, System Safety Engineer, 5375 Marple Road Suite 151, Dahlgren, VA 22448-5155, USA, telephone - (540) 653-7881, email - michael.zemore@navy.mil.

Mr. 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.

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

NSWCDD-PN-14-00339 is approved for Distribution Statement A:
Approved for Public Release; distribution is unlimited.

Ms. 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.