Understanding and Applying Total System Risk Summing
(As Outlined in the Risk Summing Guidebook)

William T. Edmonds, CSP, Headquarters Army Materiel Command, Redstone Arsenal, Alabama, USA

P. L. Clemens, PE, CSP, A-P-T Research, Inc., Huntsville, Alabama, USA

Tom Pfitzer, President, A-P-T Research, Inc., Huntsville, Alabama, USA

R. G. Baker, Chief Analyst, A-P-T Research, Inc., Huntsville, Alabama, USA

M. A. Emery, Senior System Safety Engineer, A-P-T Research, Inc., Huntsville, Alabama, USA

Abstract

System safety, in majority practice, does not assess whole system risk. Instead, as most often applied, system safety subjectively assesses the separate partial risks of individual hazards identified as posing risk to valued assets. Risk acceptance authorities then judge the acceptability of whole system risk based exclusively on their consideration of these numerous partial risks. As a result, systems are committed to operation with acceptance of whole system risk but without knowledge of its overall value. This shortcoming has long been recognized, but has gone without remedial attention in the standards guiding practice of the discipline. Risk Summing ideas and techniques applied in routine system safety practice date back to 1972. This paper incorporates some of the early concepts and strategies as well as more recent research and case studies. In 2005, an international risk summing workshop arrived at consensus on criteria for a risk summing method. Such a method, now developed and described herein, satisfies requirements for simplicity, universal applicability, and interpretability of results. In addition to summing, it recognizes a family of aids for characterizing and interpreting total system risk. Opportunities for conservation of resources while lowering overall system risk are also made apparent.

Introduction

The mission of the Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs (ATP) Task Force is to investigate and recommend or implement changes to policies, procedures, initiatives, education and training, and investments to ensure that acquisition programs address safety throughout program life cycle. DSOC funded development of the Risk Summing Guidebook (ref. 1) to provide the system safety community with a means to generate and communicate whole system risk. This paper provides a summary of the Risk Summing Guidebook and details for using the methodology and process defined by the guidebook. In addition, the guidebook contains background information, supplementental information, and practical worked examples and should be used to obtain more detail and explanations.

The Need

In today's most prevalent mode of system safety practice, the assessment of system risk begins by identifying system hazards, i.e., the sources of potential harm to identified assets. These individual hazards are then analyzed singly as line item entries in an inventory. The process can be modeled by a multiple path flow representation, as in Figure 1. Here, the system safety analyst first examines the individual hazards (H_1 through H_n) as to the severity of the harm that each would be expected to inflict (S_1 through S_n), and these data are recorded. Similarly, the probability that harm at that level of severity might occur is examined and recorded (P_1 through P_n).The analysis product is a line-item inventory of individual system hazards and their risk, as arrived at subjectively.

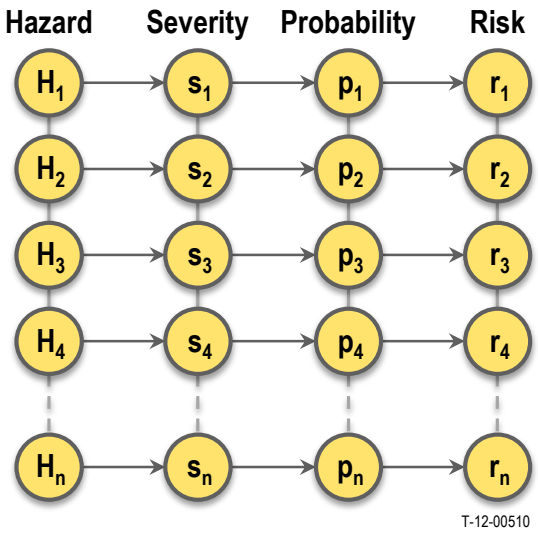

Figure 1 — Conventional Risk Assessment

Next, the analyst consults a risk assessment matrix to establish the level of risk posed by each hazard. Such matrices are found in many system safety standards, e.g., references 2 and 3. The standards provide interpretive phrases as guides to judging the severity and probability values to be assigned to the hazards. This approach has been followed in the majority practice of system safety since the 1970s (ref. 4). Figure 2 provides a bar chart model of a result of a portion of a risk assessment. Heights of bars r_1 through rn indicate the quantitative values of the risk for the hazards that each represents. Risk r_4 extends above a Risk Tolerance Limit as set by the System Safety Program Plan or an equivalent document. System Safety Program Plans typically require that hazard risk be mitigated in such cases to draw their residual risk below the Risk Tolerance Limit. However, it still remains for the Risk Acceptance Authority to pass judgment on whether or not to accept whole system risk. The problem then is that neither the analysis nor the risk acceptance authority has developed or seen an expression of true total (whole) system risk.

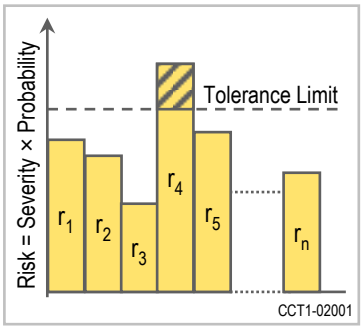

Figure 2 — Bar Chart Paradigm

The clear need is for a method to enable viewing summed total system risk in addition to the familiar partial risk inventory now in use. Ideally, that method would satisfy certain criteria:

- Consensus Requirements — In a 2005 international workshop on risk summing methods (ref. 4), a number of risk summing methods were reviewed. Minimal requirements for such a method were arrived at by consensus. There was accord that such a method should satisfy needs for: *simplicity; universal applicability; and ready interpretability of results.*

- Conservatism/Pessimism — If, in order to achieve simplicity, a method should incorporate opportunities for analytical errors, then those *errors should result in higher rather than lower representations of total risk.*

- Quantification — The method should be one which expresses its results numerically.

The Total System Risk Summing Approach

The Hazard Identification, Risk Assessment, Risk Acceptance and Risk Reduction Safety Process is illustrated in Figure 3. If Total System Risk Summing is added to the Risk Process Assessment part of the process the analyst and the risk manager have an opportunity to appreciate both the complete inventory of partial risks and the effect of their individual contributions to the summed total. Since the System Safety Process is iterative, the Total (whole) system risk is evaluated and reevaluated as hazards and risks are mitigated and refined.

A risk summing approach should fit into the accepted generic system safety process. Some desired characteristics of a practical risk summing method would be a method that:

1) is easy to use,

2) defines total risk by calculable results that are characterized in a practical way,

3) provides results that have interpretability,

4) provides results that have broad applicability.

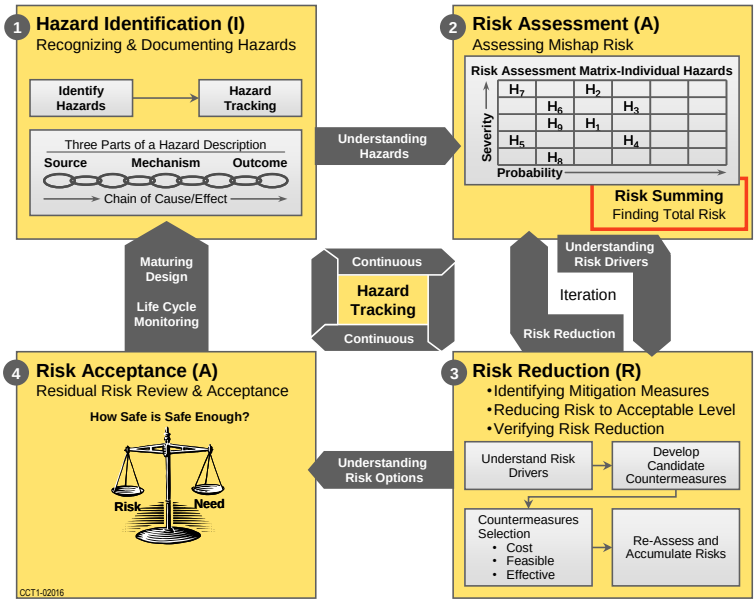

Figure 3 — System Safety Process with Risk Summing

The Step by Step Process

The major steps in performing system risk summing are presented in Figure 4 below. The process was separated into the analytical steps and management steps. This paper will focus on Analytical steps 4 and 5 letting the reader refer to the Risk Summing Guidebook (ref. 1) for explanations of Analytical steps 1, 2, 3, and 6 as well as the Administrative Steps A, B, and C. However, it is important to point out that step A in the Administrative section is the step to set total system risk limits. These limits would be unique to each evaluated system and would be set by the risk acceptance authority. Once a standard is set for guidance, these limits would be tailorable.

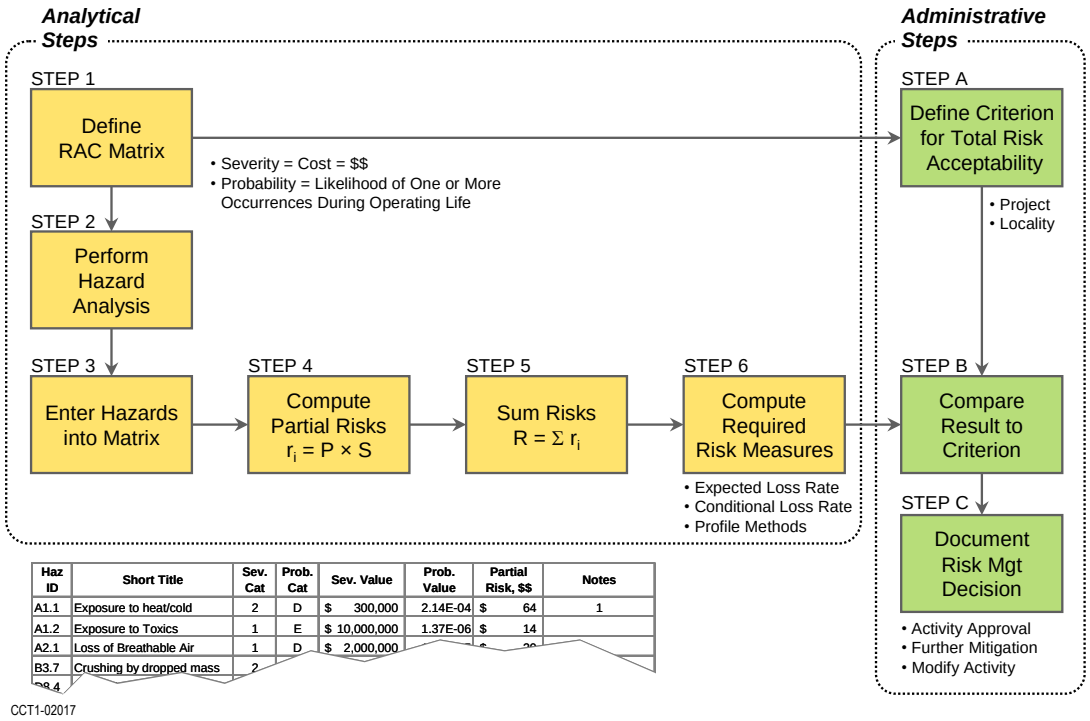

Figure 4 — Risk Summing Process

Quantifying Total System Risk

Risk assessment matrices are almost universally used by system safety practitioners in determining risk for individual line-item hazards. Dimensioned numerical values are used to scale the severity and probability axes of many standard-sanctioned risk assessment matrices (e.g., refs. 4 and 5). Thus it becomes possible to attach quantitative expressions to hazard-by-hazard declarations of both probability and severity. Using those numerical expressions, advantage may be taken of the risk-defining relationship developed by Blaise Pascal and others during the early 17th century Baroque period. Despite occasional attacks by doubters, the relationship continues in widespread and successful use, most particularly in such hugely profitable enterprises as insurance underwriting, casino gambling, and lotteries. The partial risk posed by each identified hazard is the simple product of the expected loss incurred if the hazard produces a mishap and the assessed probability that a loss event will occur as noted in Analytical Step 4. The relationship has both great simplicity and intuitive appeal:

$$r_i = \text{Partial Risk} = \text{Severity} \times \text{Probability} \tag{1}$$

Step 5, the risk summation task, is further defined by the mathematical expression and expanded equation as follows:

$$R_T \approx \sum_{i=1}^{i=n} r_i = r_1 + r_2 + r_3 + \ldots + r_n \tag{2}$$ [1]

where:

R_T = Total Risk
r_i = Partial risk = Hazard Severity × Hazard Probability

[1] The approximate expression shown here is used throughout in the interest of simplicity. Its use produces a numerical result that is very slightly larger in value – i.e., pessimistic – when compared to an exact solution. Such substitutions, often used in system safety practice, are known as "rare event approximations."

This equation can be expanded to accommodate risk for numerous threatened assets exposed in varied operational or mission phases:

$$R_T \approx \sum_{k=1}^{k=n} \sum_{j=1}^{j=m} \sum_{i=1}^{i=l} (r_{ijk} = s_{ijk} \times p_{ijk}) \quad (3)$$

where:

- R_T = the total risk posed by all identified hazards to all threatened assets during the system's complete life cycle.
- s_{ijk} = severity of the injury/damage that the i^{th} identified hazard may produce in the j^{th} asset under threat during the k^{th} mission phase under consideration.
- p_{ijk} = the probability that the consequence described by s_{ijk} is produced in the specified asset by the specified hazard during the specified mission phase.
- r_{ijk} = the partial risk posed by the i^{th} identified hazard to the j^{th} asset under threat during the k^{th} mission phase under consideration.

Important Assumptions

Three important assumptions are made in applying the approach implicit in equation 3. First, it is assumed that all identified hazards are statistically independent, meaning simply that no identified hazard can cause nor be caused by another. Secondly, multiple hazards within a system sometimes share a common outcome. Because partial risks that form these Boolean unions are simply summed, an error arises in the final total probability for that shared outcome. This error, however can be assumed to be both quite small (i.e., much smaller than errors introduced in making probability estimates) and pessimistic (i.e., producing larger rather than smaller values of total probability). The procedure is akin to the rare event approximations made in summing fault tree OR gated probabilities. This matter is discussed further in reference 6 sheets 87-5 and 87-6. Moreover, studies have shown that first-pass analyses using such line-item methods as preliminary hazard analysis leave 20-40 percent of system hazards undiscovered (ref. 7). Pessimistic errors can partially offset this deficiency.

Lastly, it is axiomatic that the sum of all system partial risks cannot be found unless all system hazards have first been identified. This logic would seem to be of trivial importance. However, recent work has shown than it is rare for more than 80% of the total of all significant system hazards to have been identified prior to committing a system to service. This matter is discussed at length in reference 8, where recommended means to combat the problem also appear.

Four Practical Total System Risk Descriptors

While the Total System Risk, computed above, is the primary summed risk measure used to determine acceptance, the International Risk Summing Workshop identified five approaches for communicating and displaying total risk using a RAC matrix. Four of these summed risk measures are characterized as descriptors which provide expected loss rate, conditional loss rate, and two profiling methods. These descriptor methods were subsequently described in a paper published in the Journal of System Safety (ref. 4) as well as documented in the Total System Risk Summing Guidebook and thus are not described in this paper.

Applying Total System Risk

Almost exclusively, the probabilities of hazards identified in Preliminary Hazard Analyses, Failure Modes and Effects Analyses, and other hazard inventory techniques are statistically independent of one another (exceptional cases are readily recognized and dealt with using alternate analytical methods). However, mathematical expressions used in the guidebook to illustrate the summing process assume that hazard probabilities are mutually exclusive. Developers of the summing method found in the guidebook made a deliberate decision to adopt this approach as a means for gently introducing the novice practitioner to the need for summing and to a simplified method for carrying it out. The mathematics apparent in the equation of the guidebook is immediately recognizable to the beginner as those of simple summation. The result of its use is one of several that are known as "rare event approximations." The error introduced in this case is a pessimistic one -- i.e., the indicated risk exceeds the true risk

by a very small amount. Thus, it partially offsets the inevitable error introduced by neglecting to inventory all system hazards.

Purists in probabilism will be quick to recognize that the form of the equation is incorrect when applied to instances of statistically independent hazards. An exact expression is appreciably more complex in appearance and would be expected to be off-putting to the summing newcomer. It is proposed to introduce and to apply -- in a future revision of the guidebook -- the more complex expression that leads to an exact solution in place of the current equation. Development of an automated tool that performs the complex computations transparently is also an option.

In another deliberate probabilism shortcut, hazards threatening more than one asset are considered in the guidebook to constitute multiple hazards and not as single initiating root events, each having multiple discrete consequences. The former enables the simplification represented by the equation, whereas the latter requires use of multiple conditional expressions. This simplification, again, can only result in a slightly higher-than-true value of overall risk. This simplification, too, would be eliminated in a future edition of the guidebook in the interest of summing "purity."

Although tailoring of the risk assessment matrix is permitted by MIL-STD-882D (§ A.4.3.2), it is not often practiced. When correctly applied, matrix tailoring optimizes the resolution capability of the matrix by adjusting both the span and the indices of the scaled axes. Thus, it becomes a useful companion tool for use in support of summing. Total System Risk Summing should be easily incorporated into electronic hazard tracking systems and electronic risk management tools. The addition, or deletion, of each hazard (partial risk) should drive the Total System Risk to change in some way which should be available in the output of the tool.

Anticipated Objections

Seasoned professional system safety practitioners are a generally wary group. They have reason to be suspicious of new, untried, and unproven analytical methods. They've witnessed gimmicky flash-in-the-pan failures in the past, and risk summation may be seen as just another one. Here are a few anticipated objections to adopting whole system risk summation. Following each are counterarguments to be considered when pondering the objections.

Potential Objection 1: Nobody's asking for summed risk, and nobody's teaching it, or using it, and nobody knows how to interpret the results.

Response 1: True — and all of those things were equally true of fault tree analysis before 1960 and true also of failure modes and effects analysis before 1949. Both of those analytic tools are now widely requested, taught, used, and producing interpretable results. It's true that interpreting whole-system risk analysis results will pose an interesting problem until we have accumulated experience at it. Accumulating a database of results for systems of diverse sizes and performing diverse functions will help. Progress requires change and change requires adaptation and time. Stagnation thrives without progress.

Potential Objection 2: Antiquity wins! — There is an inclination among system safety practitioners to hold fast to analytical methods that have garnered "honor" through long standing survival in field use. There is general reluctance: "We've been doing it this way for four decades, *and it has worked well!"*

Response 2: This is an inclination that has given the practice stability but has, equally, stifled progress. A lengthy record of survival alone is neither an indicator of excellence nor a justification for continued retention by the user community. The seriously flawed phlogiston theory of conflagration and oxidation (1667 –1753) serves as an outstanding example. Before its ultimate abandonment, it served for more than 80 years during which it survived both theoretical and empirical attacks. Its demise ushered in magnificent bursts of progress in both theoretical and wet-bench chemistry.

Potential Objection 3: This method will not work because the hazards are not independent.

Response 3: The total system risk summing equation to produces a pessimistic approximation compared to an exact solution similar to a rare event approximation. If the hazards are not caused by each other then they are statistically

independent. If the hazards are expressed in conventional methods that identify the source, mechanism, and outcome the overlap of non-independent hazards can be easily recognized and merged or dissociated.

Potential Objection 4: The method cannot be applied when the risk analysis is only qualitative.

Response 4: Qualitative analyses are based on a defined Risk Assessment Code (RAC) matrix. The requirement to quantify individual (partial) risks demands only that the indices of the RAC matrix be given quantitative bounds. When the risk summing process is completed, the total risk result is easily returned to the RAC matrix enabling the total risk to be portrayed qualitatively on the matrix. This consistent portrayal of results using either quantitative or qualitative means supports use of risk summing in situations where all results are communicated using a qualitative approach.

Summary

It is intended that this paper provides the analytical approach for determining total system risk. This paper clearly describes the process for summing and evaluating total (whole) system risk and provides the reader with reference points to the DSOC Risk Summing Guidebook. This analytical approach should be used by safety managers and risk acceptance authorities to determine their total summed system risk. The results of total system risk summing should assist the decision makers in determining the effect of fixing or not fixing a particular hazard and that effect on the total system risk. Potential objections to the analytical approach have been noted and rebutted as well. A future milestone is to provide risk managers and acceptance authorities with evaluation tools. These evaluation tools could aid in setting total (whole) system risk limits and evaluating the economical impacts and comparisons of individual hazard mitigation reductions.

References

1. A-P-T Research, Inc. for Concurrent Technologies Corporation; *Risk Summing Guidebook;* Document No. CCT1-02000; August, 2011.

2. U.S. Department of Defense; *Military Standard — Department of Defense Standard Practice — System Safety;* MIL-STD-882D; February 2000.

3. TechAmerica; Standard Best Practices for System Safety Program Development and Execution; GEIA-STD-0010; February 2009.

4. Swallom, Donald W. and Clemens, P. L.; *Summing Risk — An International Workshop and Its Results;* Journal of System Safety, November-December, 2005, Vol. 41, No. 6.

5. Clemens, P. L.; *Preferences in Interpreting the Risk Assessment Matrix*; Professional Safety, June 1995.

6. Clemens, P. L.; *System Safety Scrapbook*; Tenth Edition; September 2004.

7. Cantrell, Susan and Clemens, P. L.; *Finding All the Hazards;* Professional Safety, November 2009.

8. Pfitzer, Tom and Clemens, P. L.; *Risk Assessment and Control — Is Your System Safety Program Wasting Resources?;* ASSE Professional Safety, January 2006.

Author Biographies

William T. Edmonds, CSP, Headquarters Army Materiel Command, 4400 Martin Road, Redstone Arsenal, AL 35898, USA, telephone – (256) 450-6518, e-mail – bill.edmonds@us.army.mil.

Mr. Edmonds currently serves as a senior safety engineer for the United States Army Materiel Command located at Redstone Arsenal, Alabama. He is a graduate of Auburn University with a Bachelor of Industrial Engineering and a Certified Safety Professional with over 25 years of system safety experience in both private industry and government service.

P. L. Clemens, PE, CSP, A-P-T Research, Inc., 4950 Research Drive, Huntsville, AL 35805, USA, telephone – (256) 327-3707, e-mail – patclemens@bellsouth.com.

Pat Clemens is a Fellow Grade member of the System Safety Society and the author/co-author of more than 30 published papers dealing with safety engineering topics.

Tom Pfitzer, President, A-P-T Research, Inc., 4950 Research Drive, Huntsville, AL 35805, USA, telephone – (256) 327-3388, e-mail – tpfitzer@apt-research.com.

Tom Pfitzer is founder and President of APT Research. He holds a Master's Degree in Industrial Engineering (System Safety Option) from Texas A&M University. He is a graduate of the US Army Intern Program in Safety Engineering and has 38 years of experience in the safety field. He has been recognized by the System Safety Society as National Manager of the year for his efforts to bring common practices to the areas of System Safety, Range Safety, and Explosives Safety.

R. G. Baker, Chief Analyst, A-P-T Research, Inc., 4950 Research Drive, Huntsville, AL 35805, USA, telephone – (256) 327-3371, e-mail – bbaker@apt-research.com.

Bob Baker is a member of the System Safety Society and the author/co-author of numerous papers in the areas of flight safety, explosive safety, and system safety.

M. A. Emery, Senior System Safety Engineer, A-P-T Research, Inc., 4950 Research Drive, Huntsville, AL 35895, USA, telephone – (256) 327-3396, e-mail – memery@apt-research.com.

Melissa is a member of the System Safety Society and the author/co-author of several papers in the area of System Safety.