A mathematically guided strategy for risk assessment and management

A. Cooper
Sandia National Laboratories, U.S.A.

Abstract

Strategies for risk assessment and management of high consequence operations are often based on factors such as physical analysis, analysis of software and other logical processing, and analysis of statistically determined human actions. Conventional analysis methods work well for processing objective information. However, in practical situations, much or most of the data available are subjective. Also, there are potential resultant pitfalls where conventional analysis might be unrealistic, such as improperly using event tree and fault tree failure descriptions where failures or events are soft (partial) rather than crisp (binary), neglecting or misinterpreting dependence (positive, negative, correlation), and aggregating nonlinear contributions linearly. There are also personnel issues that transcend basic human factors statistics. For example, sustained productivity and safety in critical operations can depend on the morale of involved personnel. In addition, motivation is significantly influenced by “latent effects,” which are pre-occurring influences. This paper addresses these challenges and proposes techniques for subjective risk analysis, latent effects risk analysis and a hybrid analysis that also includes objective risk analysis. The goal is an improved strategy for risk management.

Keywords: risk analysis, assessment and management, safety engineering, latent effects, hybrid analysis.

1 Introduction

Risk assessment and risk management can be facilitated by appropriate quantitative analysis techniques. Unfortunately, “conventional” probabilistic and statistical analyses usually depend on objective inputs, and these are generally scarce. Classical techniques help understand how to solve problems analogous
to the probability of the sum of two dice being seven, or the probability of two heads in four coin tosses. These types of techniques work well when the processes are objective. However, most real-world risk problems involve subjective data. In fact it is not uncommon for most of the information pertinent to a risk analysis to be subjective.

In general, risk analysts are taught to handle problems analogous to fair dice and fair coins and then are given on-the-job problems that are more similar to loaded dice and bent coins. New techniques are proving helpful in dealing effectively with quantitative analyses that incorporate subjective information. This does not mean that objective analyses should be replaced by subjective analyses. There is usually a role for both, combined if possible in “hybrid” analyses. This is somewhat analogous to “seeing” a three dimensional object in more than one two-dimensional photograph. Additional perspectives can be helpful.

Some of the analytical challenges that can be met or partially met through subjective analysis techniques are:

1. The likelihood of severe and rare accident environments is difficult to predict because of the rarity with which these are experienced and the difficulty of determining how “credible” rare environments are. Interestingly, there is evidence that analysts tend to underestimate such risks [1].
2. Component failures are not always binary. For example, components can lose some functionality, can give intermittent problem indications, and can fail or apparently be on the verge of failure and then recover.
3. Some indications of problems, such as ultrasonic interior crack detection, can be ambiguous.
4. Human actions are difficult to predict. This is complicated where there are ulterior motivations, such as disgruntlement or malfeasance.
5. Pressures (e.g., time constraints) that affect inspection, repair, and maintenance can affect the quality of the work done and consequently the inherent risk.
6. Safety-culture factors, such as commitment, willingness to assume responsibility, and persistence are strong contributors to risk mitigation.
7. Other human factors, such as overconfidence in analysis, complacency due to a period of good fortune, combined with a tendency to minimize the risk potential can increase the likelihood of disaster.
8. An atmosphere of excessive fear can suppress open and frank disclosures, which can in turn hide problems, impede correction, and prevent lessons learned.
9. A cultural mind-set of commitment, attentiveness, self-responsibility, and passion for an activity is a significant predictor of an activity’s success.

Since these factors are mostly subjective, analysis approaches that are tailored to subjective information can improve the analytical ability to deal with them, as well as the inherent uncertainty. These approaches can also be combined with objective information in a “hybrid” analysis. As an illustrative example, consider the comparison of a probabilistic and a possibilistic approach to a hypothetical problem. In the problem, a golfer is known to have made six
“birdies” on the front nine holes, and an estimation of the number of additional birdies the golfer will make over the back nine holes is desired. Using a frequentist probability approach, one might estimate that six birdies will also be made on the back nine. In order to account for probabilistic variability, a binomial distribution might be assumed in a Bayesian approach in order to calculate the likelihood of \( n \) birdies, where \( 0 \leq n \leq 9 \). The calculation is:

\[
P(n) = \binom{9}{n} \left( \frac{1}{3} \right)^n \left( \frac{2}{3} \right)^{9-n}
\]

In this solution, the highest probability result for \( n \) is six, with a probability of about 0.27. The probability of no additional birdies is about \( 5 \times 10^{-5} \). Some of the problems with these types of approaches are that there is subjective uncertainty, since nothing is given in the problem about the golfer or the course. If the back nine were very difficult and the subject had been very lucky over the front nine, the probability of no additional birdies might be much higher than \( 5 \times 10^{-5} \). Objective information narrows the range of \( n \) to between zero and nine, but there is no objective likelihood that can be assigned to further narrow the possible values of \( n \) or to calculate the inherent probabilities. Given no information about the golfer or the golf course, the appropriate answer to the problem is that all numbers for \( n \) between zero and nine are possible.

Mathematically quantifying human and other soft qualitative data along with objective data helps make rational management choices among tradeoffs. In order to address these issues, a high level aggregate safety and security design and analysis model is proposed in this paper, showing how to improve treatment of a variety of these difficult factors.

The “hybrid latent effects” analysis developed in this paper is an approach for incorporating subjective analysis and for linking objective and subjective analyses. Since conventional objective analysis techniques are well known, and possibilistic techniques have been studied extensively [2], this paper concentrates on the development of subjective analysis for the above-mentioned types of soft factors, for aggregating available information into quantitative metrics that contribute to strategic management decisions, and for measuring the results. The approach also addresses the inherent uncertainties, and allows for tracking dynamics for early response and assessing developing trends. The model development is based on how latent effect factors combine and influence other factors in real time and over extended time periods. This approach can help show how potential strategies for improvement can be tested and measured, and how input information can be determined by quantification of qualitative information in a structured derivation process.

2 Possibilistic analysis

Two basic advantages of possibilistic analysis [Ref. 2] as a method of processing subjective information are:
1) It does not require assumptions about probabilities within the range of uncertainty that are not objectively known.
2) It does not artificially suppress the possibility of extreme values based on assumptions involved in the calculus of probability density functions.

The latter point can be illustrated by the addition of two variables, each of which is known only to the extent of an upper and a lower bound (similar to the previously posed golf example). Denoting the variables as \( x_1 = (a, b) \) and \( x_2 = (c, d) \), where the first entry of each pair is the lower bound and the second entry is the upper bound, a solution for \( x_1 + x_2 \) is sought. For illustration, assume that \( b - a = d - c \). If the range is described by a uniform probability distribution (the “maximum entropy” approach: “Any value is as likely as any other value”), the result is shown in the top part of Fig. 1. This is basically a convolution of all potential contributions to the sum [3]. If the range is viewed as a possibilistic function (no probabilistic information available inside the interval between the bounds), the result is shown in the lower part of Fig. 1. This is basically an interval solution for this example.

![Figure 1: Comparison of probabilistic and possibilistic processing.](image_url)

### 3 Systemic analysis strategy

A detailed analysis strategy was developed, as described below. In summary, the basic approach is to first perform a hazard identification to discover potential problems. This allows a high-level latent effects mathematical model to be constructed (described subsequently). Then a hazards criticality analysis is done to show the extent and safety impact of each hazard and to measure the associated range of seriousness. The combination of hazards analysis, criticality analysis, and decomposition allows ranking areas of concern. Then event trees
are constructed to show various relatively immediate contributions to failure or malfunction. With this information, high-level deductive fault trees are constructed. The availability of a latent effects model, fault trees, and event trees allows determination of the appropriate inputs needed to perform the analyses. Data are applied in a hybrid analysis to event-tree and fault-tree structures and to the latent effects model in order to measure the potential for failures of various types and their seriousness. The analysis results are the outputs of the latent effects model (along with the attendant importance, sensitivity, and early alerts), and the outputs of event trees and fault trees (probabilistic, possibilistic, or qualitative).

This process is iterative as information and results are obtained. The overall framework utilizes a strategic combination of a latent effects decomposition, hazards identification, hazards criticality, event trees, and fault trees, as described above. This strategy is depicted in Fig. 2.

![Figure 2: Process constituents and interrelations.](image)

The general decomposition approach development follows the “DIAL” (decomposition, information, analysis, learning) process (Figure 3) using first “red thinking” (what can go wrong) and then “blue” thinking (what the intended functionality and mitigating controls are) [4]. The decomposition is guided by the latent effects model, using hazards identification, hazards criticality analysis, fault trees, and event trees, all at a high level, and all including soft and possibilistic constituents. The objective is to demonstrate the feasibility of a new approach that might have merit as a supplement for existing assessment efforts.

The fault tree and event tree constructions used are for a need similar to root cause analysis. However, they differ from trees used in conventional safety analyses, which are usually based on crisp reliability-based logic (events either occur or do not occur), and for which events aggregate based on Boolean or propositional logic. Many factors (e.g., safety-culture mind-set and job commitment) vary continuously and do not fit this model. In order to fit a tree
model and obtain a probabilistic estimate, extensive data would be required on failure rates. However, a component might function with less than capability, might develop “sluggish” response characteristics, might have intermittent failures, and might be intermittent. These “soft failures” illustrate some of the limitations of crisp-logic-based fault trees and event trees. Fuzzy logic and possibilistic logic analyses are examples of techniques that can account for degraded failure in addition to full failure. Subjective data require a hybrid processing technique involving “soft aggregation” and “possibilistic” mathematics [5].

4 Markov latent effects model

A Markov Latent Effects Model (architecture, inputs, weights, dependence, and output analysis) is described in this section. “Soft” influences can bring quantitative metrics and complex interrelations to bear on assessment of the operational aspects of an organization (management philosophy, communication venues, personnel commitment, selfless sharing, etc.). This can be done through a “latent effects decomposition” (illustrated at a high level in Figure 4) that begins with the overall environment tailored to an operation, introduces an overall strategy for establishing a top-to-bottom design, demonstrates specific implementations to support the strategy, and includes operational factors for monitoring performance that support the overall approach. In addition to being a systemic approach, this also provides the framework for a comprehensive mathematical analysis.

All of the inputs have quality values (with uncertainty) and weights. The weights, which sum to one for each module, indicate the relative significance of the factors considered as inputs. Weights for inter-module connection indicate the relative significance of “secondary” inputs generated by a module. Each input is specified subjectively in the range of zero to one, including uncertainty and dependence. The mathematical computation used is a variation on the

Figure 3: Dial process.
weighted sum of inputs multiplied by the corresponding weights and added linearly (Eq. 2).

\[ y_j = \sum_{i=1}^{n} w_i x_i \]  

where \( y_j \) is the result for module \( j \), \( w_i \) is the weight for input \( i \), \( x_i \) is the value for input \( i \), and \( n \) is the number of inputs to module \( j \). This approach has the desired mathematical properties, i.e., it assures that the module outputs are also in the range zero to one, the output cannot be larger than the largest input or smaller than the smallest input; and if all inputs are the same, the output will be the common value.

However, we have found that linear weighted sums do not strictly match human decision processes, which are more closely tied to “soft aggregation” [5]. The form of soft aggregation we used treated each group of input values by a modified nonlinear weighted sum to provide an assessment score for each module, and this process continues until an overall assessment score is derived. Soft aggregation also satisfies most of the mathematical attributes given above for linear weighted sums. Input uncertainty (possibilistic or interval functions for each input) is allowed, and the results reflect this uncertainty. The modification of the weighted sum process is derived according to the nonlinear expression in Eq. 3.

\[ y = \frac{1}{1 + e^{-5.5\left(\sum_{i=1}^{n} w_i x_i - 0.5\right)}} \]  

A plot of the function is shown in Fig. 5, where the weighted sum is the abscissa, and the ordinate is \( y \).
The relevance of this analysis approach is that safety-performance can be measured (including portrayal of the inherent uncertainty), contributors to overall success can be identified through a ranked list, the most cost-effective or resource-effective areas for improvement can be similarly shown, the potential benefits of a variety of decisions can be measured, trends can be tracked, and early alerts can be constructed for proactive management action.

The derivation of mathematical metrics for subjective inputs follows an expert elicitation procedure. The input guidance is that numbers in the approximate range of 0.0 to 0.2 represent a situation that is “unacceptable,” numbers in the approximate range of 0.2 to 0.4 represent “poor,” numbers in the approximate range of 0.4 to 0.6 are “average,” numbers in the approximate range of 0.6 to 0.8 are “good,” and numbers in the approximate range of 0.8 to 1.0 are “excellent.” Uncertainty (due to multiple expert opinions or due to unsure values) is represented by intervals (lower and upper bound), or more generally, by possibilistic functions. Eq. 3 can be used for deriving lower bounds of results from the lower bounds of the operands and upper bounds of results from the upper bounds of the operands.

5 Hybrid analysis constituents

The three types of metrics concerning system safety form the basis for the output modes. Two of these are related to the probability of system failure; one an objective measure based on measured data, and the other a subjective measure based on expert engineering judgment. These are combined in an objective/subjective probabilistic hybrid analysis [6]. The third is the Markov Latent Effects measure of organization robustness with respect to safety, and is somewhat analogous to a “grade” that a student might receive in a class.

5.1 Objective measure of probability of system failure

Objective data can help give information about the probability of system safety failure. Since it is common to have some objective variability associated with
systems, the probability of failure can be described by probability density functions. Most conventional risk analysis methods give a result similar to objective probability of system failure, representing uncertainty by probability distributions as well. This concept is used here for one constituent of output, but is limited to objective variability.

5.2 Subjective measure of probability of system failure

Subjective measures are almost always necessary in order to supplement objective measures. This requires expert judgment solicitation, which is converted to fuzzy or possibilistic measures of uncertainty about the probability of system safety failure. The possibility of uncertain failure probabilities is a second constituent of output. Possibilistic probability was used rather than direct possibility in order to better match purely objective measures as well as potential requirements. The hybrid analysis that links objective probability and subjective probability determines the amount of subjectivity, so that output displays of the two are linked by the proportionate amount of subjectivity and objectivity inherent in the results.

5.3 Measure of the system organizational and operational safety status

System safety is not independent of the manner in which the system is operated, the restrictions placed on that operation, or the manner in which the operation is subjected to periodic safety reviews. These factors can be determined through a collection of metrics that form the basis for an “inspection” activity and transcend the measures of failure probability to give indicators about the safety health of the system operation. The aggregation of the data collected by inspection give a system safety “grade,” and can also lead to useful information about how to improve the system and how to gain efficiency in the inspection activity. This type of information is the third output constituent.

6 Conclusions

Possibilistic analysis and the Markov Latent Effects Model provide an effective supplement to conventional safety analysis approaches and are a crosscheck on conventional deficiencies. One of the most important ways to prevent disasters is to become more sensitive to the importance of factors that the model can process, such as personal culture, precursor indications, and soft failures. Future work will address these areas in order to validate a full Markov Latent Effects Model.

Acknowledgments

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.
Many people assisted in this effort with suggestions and supporting information, including Scott Ferson (Applied Biomathematics), Paul Werner, Dick Perry, Dennis Roach, Bob Roginski, and John Covin (all of Sandia National Laboratories), and Prof. Tim Ross (University of New Mexico). The work was funded by the NNSA LDRD Program and by the FAA, Aging Mechanical Systems Program.

References