Abstract

This paper improves on some of the limitations of conventional safety assessment and decision analysis methods. It develops a top-down mathematical method for expressing imprecise individual metrics as possibilistic or fuzzy numbers and shows how they may be combined (aggregated) into an overall metric, also portraying the inherent uncertainty. Both positively contributing and negatively contributing factors are included. Metrics are weighted according to significance of the attribute and evaluated as to contribution toward the attribute. Aggregation is performed using exponential combination of the metrics, since the accumulating effect of such factors responds less and less to additional factors. This is termed “soft” mathematical aggregation. Dependence among the contributing factors is accounted for by incorporating subjective metrics on “overlap” of the factors and by correspondingly reducing the overall contribution of these combinations to the overall aggregation. Decisions corresponding to the meaningfulness of the results are facilitated in several ways. First, the results are compared to a soft threshold provided by a sigmoid function. Second, information is provided on input “Importance” and “Sensitivity,” in order to know where to place emphasis on controls that may be necessary. Third, trends in inputs and outputs are tracked in order to add important information to the decision process. The methodology has been implemented in software.

Introduction

There are important situations in decision analysis in general and safety assessment in particular that must be judged by weighing a variety of diverse factors that are uncertain and do not combine linearly or independently. Conventional mathematical models that can combine factors directly or through propositional logic to derive metrics (e.g., probabilistic risk) are insufficient for these classes of problems. For example, the safety status of an airline operation might depend on measuring factors such as accident/incident statistics, maintenance personnel/pilot competence and experience, scheduling pressures, and safety “culture” of the organization. Many of the potential metrics on such individual parameters are difficult (and generally uncertain) to determine. A top-down analytical approach requires more than individual parameter assessment, which is used in some tabular schemes. Furthermore, aggregation of the parameters into an overall metric requires a methodology that can account for nonlinearities and dependence. For example, twice as many attributes is unlikely to be twice as beneficial, and scheduling pressures could influence accident/incident statistics.

Methodology that can address this problem has been developed based on soft aggregation. Soft aggregation accumulates information nonlinearly and combines it in order to measure an attribute of a system (e.g., safety) or to test hypotheses (e.g., for forensic deduction or decisions about various system design options). An important application of the methodology is in measuring and portraying uncertainty concerning attributes such as system safety that require accumulating various subjective metrics, especially where there are ill-defined interrelations among the contributors. We will describe an example application in the field of airline safety. This approach can also be combined seamlessly with conventional approaches. In other words, an overall system might be decomposed into constituent subsystems, some of which are treated by linear mathematics, some by propositional logic, and some by soft aggregation.

* 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.
The technique extends naturally to decision analysis, where decisions must be made about acceptability of system safety or about the need for operational restrictions; and also to selection among alternative approaches or forensic hypotheses.

In this work, we have carefully observed the attributes of conventional methodology with the intent of eventually developing a seamless interaction or overlay. Our objectives include:

- deriving safety performance metrics
- facilitating decision analysis
- prioritizing safety hazards
- prioritizing hazard controls
- helping determine proper response actions

**Soft Aggregation**

Soft mathematical aggregation is useful in a significant number of applications. Inputs may contribute to the output without being related to linear, Boolean, or possibilistic mathematics. For example, a production line employee who is disgruntled or unmotivated, or a training program that is not done skillfully might not directly contribute to an accident, but the presence of such situations projects safety concerns and potential contributors to an accident, if other unfavorable events occur.

As another example, a medical doctor may accumulate weighted health information combined non-linearly (weight/height, blood pressure, temperature, pulse rate, blood test parameters, reflexes) to indicate the patient’s state of health. Safety indicators are similar. The potential effectiveness of protective measures (e.g., medicine) is also weighed. In these and similar applications, there is a particular need for contributions that push toward a limit (e.g., “unsafe” or “safe”) without ever being assured of reaching the limit. Our model for these situations is exponential, as shown in Figure 1. Safety protective measures are aggregated up the ordinate and threats are aggregated down the ordinate. The abscissa indicates a weighted “rating” function that is subjectively obtained and based on expert judgment. The equation used is:

\[ f = \left[ 1 - e^{-\sum_{i=1}^{n} w_i x_i} \right] \left[ e^{-\sum_{j=1}^{m} v_j y_j} \right] \]  

(1)

The \( w_i \) and \( v_j \) indicate “weights” on the significance of the protective measure and threat aggregates, respectively (\( n \) and \( m \) in number). The weights are normalized so that \( \sum_{i=1}^{n} w_i = 1 \) and \( \sum_{j=1}^{m} v_j y_j = 1 \). The \( x_i \) and \( y_j \) are ratings of how good the controls are and how bad the hazards are on a scale of 0 to 1. The constant \( k \) is a variable dependent on the number of aggregate constituents. The figure shows an example aggregation of threats and controls. The aggregation can be carried out with the parameters combined in any order; or the aggregation can be carried out for the entire system.

![Figure 1. Exponential Aggregation with Threshold of Concern](image)

We frequently delude ourselves into thinking thresholds of concern, such as probabilistic safety requirements, are firm, whereas their source is not firm. For example, if we have a requirement that a system must maintain safety from catastrophic failure to a probability of one in a million, the implication is that an analysis that derived a system safety measure of \( 1 \times 10^{-6} \) would be indicative of a satisfactory system (meets the requirement) and an analysis that derived a system safety measure of \( 1.1 \times 10^{-6} \)

\[ 1\times10^{-6} \]
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.
would be indicative of an unsatisfactory system (fails to meet the requirement).

In order to more realistically portray the comparison of information aggregation with a threshold of concern, such as that portrayed in Fig. 1, we postulate a non-abrupt transition. This process is termed a "sigmoid," and is expressed as an exponential function that transitions gradually from zero to one as an abscissa value $x$ increases through zero, with a transition rate determined by a constant, $c$. Figure 2 shows an application of this idea to "threshold logic," where weighted sums are compared to a threshold to realize a Boolean function. The transition constant shown is $c = 1.5$.

$$f = \left( \frac{1}{1 + e^{-cx}} \right)$$

**Figure 2. Sigmoid Transition for Threshold Logic**

**Implementation Methodology**

The implementation strategy is shown in Figure 3 for the highest level of use. The inputs to the system function can have positive or negative effects as shown by entry into the function through circles (indicative of "hazards") or straight lines (indicative of "controls").

**Figure 3. Top-Level Functionality**

Inside the function box is indication of accumulation of inputs as time progresses, and the potential to build to a critical level of concern (determined by a decision threshold) at any time. The outputs are the basic system status (e.g., a measure of safety), Importance and Sensitivity information about the inputs, trends (for inputs and outputs), and actions (response taken because of information provided).

Each function can be decomposed into subfunctions to an arbitrary level. In our applications, we offer selectable levels of decomposition. As example is shown below decomposed into four subsystems.

**Figure 4. More Detailed Decomposition**

**Possibilistic Uncertainty**

Because inputs are not generally known specifically (subjectivity is usually involved) traditional methods of portraying variability (e.g., probability distributions) must be supplemented with methodology that is specifically tailored to processing subjective uncertainty (e.g., possibilistic mathematics). Our methodology uses fuzzy mathematics [1].

Fuzzy mathematics is a form of possibilistic processing. The difference between fuzzy logic and fuzzy mathematics is roughly analogous to the difference between Boolean algebra and the algebra of real numbers. Like probabilistic calculus, fuzzy mathematics also can be applied to introduce variability to fixed parameters. For example, a subjective parameter can have some of the characteristics of more than one number (e.g., "approximately" five may indicate a range of real numbers including, but not limited to, five). Fuzzy models can therefore be applied to...
describe parameters in analyses (e.g., probability analysis), and this has some similarity to strictly conventional descriptions. However, fuzzy algebra differs from conventional mathematics both formally and in concept.

Since fuzzy mathematics does not assume the precise relationships inherent in probability distributions, it appears to be more appropriate for the subjective inputs applicable to vaguely defined situations.

A fuzzy number (formally a convex and normal fuzzy set) can be represented mathematically [1] as:

\[ A_\mu(x) = A_\mu = [a_1(\mu), a_2(\mu)] \]  

(2)

where the \( a_1 \) and \( a_2 \) values on \( x \) represent the lower and upper limits, respectively, of the variation possible for the parameter as a function of \( \mu \), and \( \mu \) is a "level of presumption." The level of presumption represents a collection of subjective judgments about the range specified. One must be more presumptuous in order to specify monotonically decreasing variable ranges (maximum level of presumption is presumption of minimum uncertainty).

![Figure 5. Example Fuzzy Number](image)

The concept of level of presumption facilitates assuring the convexity property. The "normal" restriction fixes the maximum level of presumption at 1 and the minimum to 0. If a particular value of presumption, \( a \), is selected, a horizontal line can be drawn that intersects the ordinate at \( \mu = a \). The two points where the line intersects the function represent the lower and upper bounds for the parameter at the specified presumption level. No information is implied within these limits.

In contrast to fuzzy logic, fuzzy mathematics treats operands as fuzzy (subjectively known) numbers with uncertainty along the abscissa, and computes in terms of abscissa values rather than ordinate values. The mathematical basis for combining fuzzy numbers is based on Zadeh's Extension Principle [2]. For addition and multiplication (basic to fault tree and event tree computations), this produces:

\[ \mu_{A+B}(x) = \bigvee_{z=x+y} (\mu_A(x) \land \mu_B(y)) \]  

(3)

\[ \mu_{A \times B}(x) = \bigvee_{z=x \times y} (\mu_A(x) \land \mu_B(y)) \]  

(4)

These are convolutions basically constructed like those used in probabilistic calculus, but without the "independent" abscissa valuations. This is because the above fuzzy-algebra operations utilize only ranges of values, and make no use of or assumptions about relationships between probability parameters, or of independence between probability parameters. The operations shown above are directly useful for parameters for which relative probabilities and independence are not well known (a common situation). On the other hand, probabilistic operations are limited to parameters for which these characteristics are well known (a less common situation). Using probabilistic methods in ill-defined situations (where fuzzy methods are more appropriate) can inappropriately reduce apparent uncertainty and may lead to incorrect decisions.

**Importance and Sensitivity**

In addition to the information provided by the output, information about the inputs is valuable. Two measures are Importance (amount of contribution to the output) and Sensitivity (amount of change in the output that a change in the input could make if improved). For Importance, we use the weighted sums generated by each input to derive the amount of contribution, and for Sensitivity, we use one minus the value multiplied by the weighted sums generated by each input to derive the amount of potential for improvement.

1 Preferably from "experts," preferably based on data (even if limited), and possibly weighted according to expertise.

2 However, treatment of independence/dependence properties is not precluded.
Trends

Static assessments are not nearly as useful as records of multiple assessments over time, from which trends can be derived. This methodology provides trends information in several ways. The inputs can be stored in a database, so that historic information can be plotted to show trends over time. The same process is used for the overall result output, and for each subsystem output.

An example trends plot is shown in Figure 6. In the figure, the quantitative representation of a particular input is tracked over a period of time, during which multiple assessments are made. As is typical of such plots, there is some noise on the plot as trends develop. Also indicated (by the vertical spread) is the uncertainty due to subjectively derived evaluations.

Figure 6. Example of Trends

Conclusions

The methodology described in this paper has many applications where data are "soft" and cannot be processed through propositional logic or linear mathematics. It has been used successfully in many of our analyses, and parts of it have been implemented in our risk analysis software.

Acknowledgments

Among those contributing ideas to this development were Perry D'Antonio, Paul Werner, John Covan, and Wayne Chick, all of Sandia National Laboratories.

References


Biography

J. Arlin Cooper, Ph. D., Distinguished Member of Technical Staff, Sandia National Laboratories, Albuquerque, NM 87185-0490, USA, telephone—(505) 845-9168, facsimile—(505) 844-9225, e-mail—a cooper@sandia.gov.

Dr. Cooper has worked for 35 years in safety and security system design and analysis. He has three patents, has authored three books and contributed to several others, as well as numerous journal publications. His Ph. D. is from Stanford University.