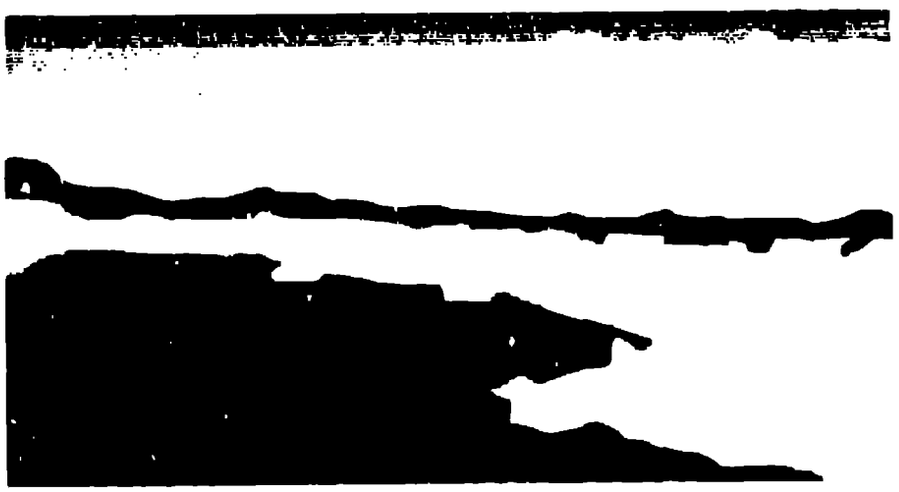
LA-UR- 93 - 1358

Title: FUZZY RISK ANALYSIS FOR NUCLEAR SAFEGUARDS

Author(s): A. Zardecki

Submitted to: Fifth International Fuzzy Systems Association World Congress, Seoul, Korea, July 4–9, 1993



Los Alamos
NATIONAL LABORATORY

Fuzzy Risk Analysis for Nuclear Safeguards

Andrew Zardecki

Safeguards Systems Group, N4
Los Alamos National Laboratory
Los Alamos, NM 87545

April 1, 1993

Risk analysis of a safeguards system, based on the notion of fuzzy sets and linguistic variables, addresses concerns such as complexity and inherent imprecision in estimating the possibility of loss or compromise. The automated risk analysis allows the risk to be determined for an entire system based on estimates for lowest level components and the component proportion. In addition, for each component (asset) the most effective combination of protection mechanisms against a given set of threats is determined. A distinction between bare and featured risk is made.

1 Introduction

The risk analysis is an essential element in the design of an integrated safeguards system.[1,2] In contrast to traditional approaches based on the probability calculus, the theory of fuzzy sets[3] provides a framework for dealing with linguistic variables; that is, variables whose values are words or sentences in a natural language.[4,5]

To conduct a risk analysis, one represents the system as a structure that has the form of a tree of nodes. The terminal nodes (leaves) of the tree are described in terms of likelihood of loss, severity of loss, and confidence factor. When the rules of fuzzy algebra are applied, each leaf is characterized by its component risk indicator. The risk indicators of the components of each parent node are then weighted by the weight factors to produce their corresponding parent's node risk indicator. This method closely follows the performance analysis model.[6]

As in the risk assessment model of Bruce and Kandel,[7] we also consider the problem of selecting the most efficient combination of safeguards mechanisms against a given set of threats. The extension of the Bruce and Kandel model consists in making a distinction between the bare and featured risk. While the former refers to the risk relative to a specific threat in the absence of safeguards options, the latter one provides a measure of risk when the optimal safeguards options are selected. Furthermore, the featured risk combines the different threats, thus leading to a single attribute for each component of a complex system. This allows one to apply the tree representation to a system in which the sets of threats and safeguards are considered.

A preliminary version of the computer code we developed consists of two separate modules. These are the parser module that translates the natural language phrases into fuzzy sets and the fuzzy set module that performs the fuzzy arithmetics. Our ultimate goal is to produce a tool combining assessment and design for a nuclear safeguards system.

2 Risk analysis model

An automated risk utility assists a risk analyst in overcoming two problems: overall complexity and inherent imprecision. The risk assessment model overcomes inherent imprecision by providing for the input of natural language estimates for imprecise quantities. The problem of overall complexity is solved by providing a composite ranking based upon exhaustive detailed decomposition. To illustrate what we have in mind, consider a diagram of a mock facility shown in Fig. 1.

*This work was supported by the U.S. Department of Energy, Office of Safeguards and Security.

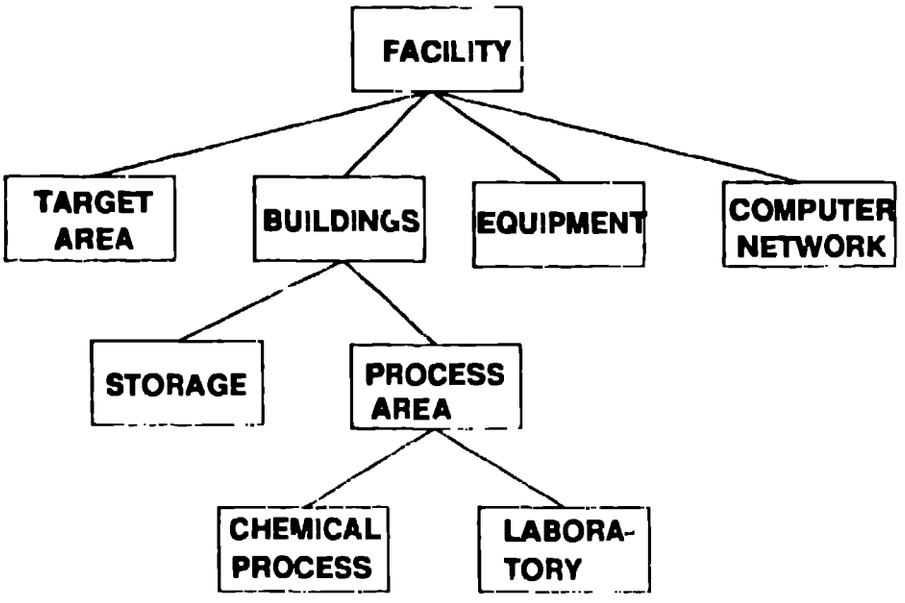


Fig. 1. Diagram for example facility

In this diagram, *Target Area*, *Equipment*, *Computer Network*, *Storage*, *Chemical Processing Area*, and *Laboratory* are the terminal nodes (components). The attributes they require are: likelihood of loss, severity of loss, and confidence factor. On the other hand, *Buildings*, and *Processing Area* are the nodes with children; their component risk indicator is computed from the three features of each child and from the weight factors attached to each link between the nodes. The component named *Facility* is distinguished by not having a parent component; it constitutes the root of the component tree.

The component risk indicator is evaluated as a fuzzy product of the three features characterizing each terminal node:

$$\text{Component Risk} = \text{Likelihood} \times \text{Severity} \times \text{Confidence Factor}. \tag{1}$$

If R_i denotes the component risk of the node labeled i, and W_i refer to the corresponding weight factors, then the risk of the parent node is given in terms of a weighted sum

$$R = \frac{\sum_{i=1}^{m} W_i \times R_i}{\sum_{i=1}^{m} W_i}, \tag{2}$$

where m is the number of nodes emanating from the parent node. Alternatively, the weighted sum could be replaced by an operation computing the fuzzy maximum, thus leading to the worst case type of description.

To introduce the notion of a fuzzy set consider a linguistic variable *Likelihood of loss*, which can take three values: low, medium, and high. As illustrated in Fig. 2, the corresponding fuzzy sets can be viewed as mappings from the set of natural or real numbers to the unit interval defining the grade of membership.

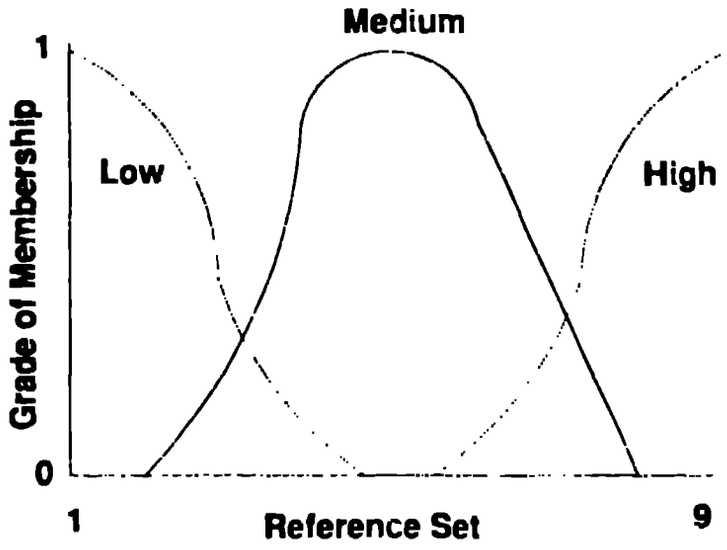


Fig. 2. Membership function for primary terms: low, medium, high.

A finite fuzzy set A having J elements on X is expressed as a symbolic sum

$$A = \sum_{j=1}^{J} \chi_A(x_j) / x_j. \tag{3}$$

This notation, which has become standard in fuzzy sets literature, indicates the grade of the membership $\chi_A(x_j)$ given x_j in the reference set. We stress that the symbolic sum is understood as a union, and that the slash symbol merely separates the membership value from the element to which the membership corresponds.

The overall risk factor should also help the analyst in locating the weakest element of the system. (For example, we could consider the fuzzy product of the component risk and the weight factor as a measure of component's importance.) Once such an element is found, the appropriate protection mechanisms that most effectively safeguard the system against a set of confronting threats will be selected. To achieve effectiveness in this area, we now turn to the model that selects the optimum configuration of safeguards based on the principle of maximum possibility.[5]

In the foregoing analysis, we tacitly assumed that each component was exposed to a single, well defined threat. In general, though, we need to broaden our focus by allowing a set of threats confronting each component of the system. For example, consider computer room as an asset we want to protect. Possible threats might include theft, fire, and unauthorized use of the computer. In such a situation, we compute the bare risk R_A^0 of the asset to each threat. The qualifier bare, denoted by the superscript zero, means that R_A^0 represents loss when no protection is provided. The priority percentage P_A, defined as the fraction

$$P_A = \frac{R_A^0}{\sum_{j=1}^{n} R_j^0} \tag{4}$$

is a fuzzy set if linguistic attributes are used: priority percentage P_k becomes numeric if the risk is computed as a simple product of the probability of occurrence and monetary vulnerability.

Assume now there is a total budget B available to protect the asset against all the possible threats. Furthermore, to each threat T_k corresponds an array M_{kj}, $j = 1,\ldots m_k$, of safeguards options (countermeasures), with m_k options available for threat T_k. To include the costs in our description, we let C_{kj} signify the costs associated with the countermeasures M_{kj}. The countermeasures M_{kj} need to satisfy restrictions imposed by three factors. First, the amount of security that each mechanism provides is different. Second, the amount of security that the system as a whole receives is the sum of securities which each mechanism provides. Third, there is a threshold cost (total budget B) that the n-tuple of mechanisms to be chosen cannot exceed. These restrictions are now expressed in terms of a possibility distribution of an ordered set of countermeasures against n threats. This possibility is given as

$$\text{Poss}(M_{1j_1},\ldots,M_{nj_n}) = 0 \quad \text{if} \quad \sum_{k=1}^{n} C_{kj} > B$$

$$= \sum_{k=1}^{n} P_k \times \text{Poss}(M_{kj_k}) \quad \text{otherwise.} \tag{5}$$

In this equation, $\text{Poss}(M_{kj})$ can be identified with the membership function of the fuzzy set representing M_{kj}. After computing all n-tuplets (there are $m_1 m_2 \ldots m_n$ of them) of the possibility distribution, we obtain a set of options and their associated costs. The set with the highest possibility is selected as the most effective set of countermeasures.

3 Featured risk

Given the array $\text{Poss}(M_{1j_1},\ldots,M_{nj_n})$ of possibility values, we can select the set of countermeasures that, for each threat gives the optimal protection. If for threat T_k, the optimal countermeasure compatibility is $\bar{M}_k$, then the bare risk R_k^B becomes dressed or featured risk $R_k = R_k^B(1 - \bar{M}_k)$. This definition recovers the bare risk if no safeguards elements are applied, that is $\bar{M}_k = 0$. On the other hand, if $\bar{M}_k = 1$, that is if the threat is entirely eliminated, the featured risk becomes zero.

The featured risk to all threats is defined as

$$R = R_1 + \cdots + R_n, \tag{6}$$

where n is the number of threats. Again, if the individual risk terms are given as fuzzy sets, the sum in Eq. (6) is to be understood as a union of fuzzy sets. We notice that Eq. (6) provides a single risk measure for each component of the hierarchical system discussed in the previous section, thus enabling one to evaluate the risk of the entire hierarchy. Compared to earlier models,[7,8] the novelty of this approach consists in inclusion of the safeguards countermeasures into the risk evaluation scheme.

4 Computational example

The theoretical considerations of Sec. 2 will now be illustrated by computing the overall risk of the example facility shown in Fig. 1. For our computation we use the data shown in Table 1.

Table I. Risk estimate of the lowest level components.

Component	Loss Likelihood	Severity of Loss	Confidence Factor
Target Area	Low	Very High	High
Equipment	Low	Medium to High	
Computer Network	Medium	Fairly High	
Storage	Low	About Three	
Chemical Process.	Fairly Low	Medium	Medium
Laboratory	Very Low	Medium to Fairly High	

The empty cells in the last column of Table I reflect the fact that the confidence factor is not a mandatory attribute of the component risk evaluation. To complete the estimation, we need to assume the proportion estimates of different components for each parent node having these components as children. Table II illustrates the proportion (weight) aspect.

Table II. Proportion estimates of different components

Parent Node	Children Nodes	Proportion
Facility	Target Area	Extremely High
	Buildings	Medium
	Equipment	Medium
	Computer Network	High
Buildings	Storage	Low to Medium
	Processing Area	Medium
Processing Area	Chemical Process.	Fairly Low
	Laboratory	High

In the actual computer implementation of the model, the linguistic data are parsed first to check if they conform to the natural language syntax. The next step is the computation of the component risk indicator for the terminal nodes, according to Eq. (1). Finally, by using the proportion estimates, we arrive at the risk indicators of higher levels. With the sample data of Tables I and II, we obtain the overall risk estimate to be medium to high.

Let us now concentrate on the computer network asset. We will arbitrarily choose a stand alone computer as the terminal node of this component of the facility to inspect. We assume the threats and countermeasures as given in Table III.

Table III. Threats and countermeasures facing the facility computer system. Note that the costs are given in terms of arbitrary units

Threats	Countermeasures	Cost
Theft	Bolting computer to the table	3
	Lock on the door	5
	Armed guards	6
Fire	Sprinkler system	4
	Fire extinguisher	3
Unauthorized use	Badge system to activate computer	3
	Access passwords	1

Table IV lists the associated compatibility array, expressed in terms of three fuzzy sets, corresponding to each threat.

Table IV. Fuzzy sets of compatibilities associated with each threat

Countermeasure / Threat	1	2	3
Theft	0.75	0.60	0.85
Fire	0.40	0.60	
Unauthorized Use	0.50	0.45	

According to Eq. (3), the three fuzzy sets C_k, which characterize the compatibilities of each countermeasure to a threat with index k, can be written as

$$C_1 = 0.75/1 + 0.60/2 + 0.85/3, \tag{6a}$$

$$C_2 = 0.40/1 + 0.60/2, \tag{6b}$$

$$C_3 = 0.50/1 + 0.45/2. \tag{6c}$$

For the sake of simplicity, we suppose the risk estimates corresponding to the three threats have numerical values 15, 20, and 35. This leads to the priority percentage values of $P_1 = 0.21$, $P_2 = 0.29$, and $P_3 = 0.50$ for three threats. Taking the total budget equal to 10 units, Eq. (5) now yields the following table for the possibility distribution of different triplets of the countermeasures.

Table V. Possibility distribution for 12 triplets of countermeasures.

Triplet	Possibility	Triplet	Possibility
(1,1,1)	0.52	(2,2,1)	0
(1,1,2)	0.50	(2,2,2)	0.53
(1,2,1)	0.58	(3,1,1)	0
(1,2,2)	0.56	(3,1,2)	0
(2,1,1)	0	(3,2,1)	0
(2,1,2)	0.47	(3,2,2)	0.58

We see that the highest possibility value of 0.58 is attained for the triplets (1,2,1) and (3,2,2). Thus if we bolt the computers to tables, install fire extinguishers, and introduce badges activating the computers, we will achieve one of the two optimal selections of countermeasures.

5 Conclusions

We provide a tool that should be useful for safeguard systems and computer security in two respects. First, an overall characteristic of a complex system is computed in terms of linguistic attributes. Second, for a selected asset, the most efficient set of safeguard mechanisms is selected. This selection includes both the budgetary constraints and the possibility distribution of countermeasures. Our future work will focus on the best allocation of resources to a complex system, following our earlier work on RAOPS, Resource Allocation and Optimization Program for Safeguards.[9]

References

1. S. B. Guarro, "Livermore risk analysis methodology: a structured decision analytic tool for information systems risk management," in *New Risks*, edited by L. A. Cox, Jr. and P. F. Ricci (Plenum, New York, 1990), pp. 301-314.
2. S. T. Smith, J. J. Lim, J. R. Phillips, R. M. Tisinger, D.C. Brown, and P.D. Fitzgerald, "LAVA: a conceptual framework for automated risk analysis," in *New Risks*, edited by L. A. Cox, Jr. and P. F. Ricci (Plenum, New York, 1990), pp. 315-330.
3. G. J. Klir and T. A. Folger, *Fuzzy Sets, Uncertainty, and Information* (Prentice Hall, Englewood Cliffs, 1988).
4. L. A. Zadeh, "The concept of a linguistic variable and its applications to approximate reasoning," Information Sciences **8**, 199-249 (1975).
5. K. J. Schmucker, *Fuzzy Sets, Natural Language Computations, and Risk Analysis* (Computer Science Press, Rockville, Maryland, 1984).
6. A. Zardecki and E. A. Hakkila, "Fuzzy methods for system performance," in Proc. 13th Annual Symposium on Safeguards and Nuclear Material Management (Joint Research Center, Ispra, Italy, 1991) ESARDA **24**, 667-670 (1991).
7. W.S. Bruce and A. Kandel, "The applications of fuzzy set theory to a risk analysis model of computer security," in *Advances in Fuzzy Sets, Possibility Theory, and Applications*, edited by P.P. Wang (Plenum, New York, 1983), pp. 351-376.
8. L.A. Stoltz and A. Zardecki, "Fuzzy risk analysis for safeguards and network security," Nucl. Mater. Manage. **XXI** (Proc. Issue.), 770-773 (1992).
9. A. Zardecki, J.T. Markin, and P. Henriksen, "Resource-Allocation Optimization Program for Safeguards, Version 2.0," Los Alamos National Laboratory report LA-12244-M (March 1992).