CONF-870713--3
BNL 39822

A SAFEGUARDS RISK APPROACH TO INSPECTION SCHEDULING*

Joseph P. Indusi
Brookhaven National Laboratory
Upton, New York USA

BNL--39822
DE87 010763

ABSTRACT

Scheduling facilities for safeguards and security inspections may be based on a relative safeguards risk ranking of the facilities under consideration. Safeguards risk is defined as a combination of the potential threat, facility vulnerability to various malevolent events, and the consequences that may occur if a malevolent event is successfully carried out. Quantification of the vulnerability (on a relative scale) and consequences may be possible, however the probability of a particular threat is impossible to estimate. The problem has been researched and an approach has been formulated which yields a relative safeguards risk ranking for a given group of facilities, malevolent events and potential threat groups. This approach may be useful in helping to direct inspection activities to high risk operations instead of being driven by a single element such as vulnerabilities or consequences.

INTRODUCTION

The scheduling of safeguards and security inspections may be approached by several rules or methods. Here we will describe an approach to inspection frequency based on the relative safeguards risk of the various facilities under consideration. The concept of relative safeguards risk as described here was originally developed in 1981-82. Prior work, theoretical in nature,

*This work performed under the auspices of the U.S. Department of Energy, Contract # DE-AC02-76CH00016.

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

was reported in "Societal Risk Approach to Safeguards Design and Evaluation", C.A. Bennett, ERDA-7, 1975. This concept to our knowledge was never successfully applied because of the difficulty in quantifying the likelihood of a threat. This fact has resulted in the approach we use here, that of relative risk ranking rather than an absolute quantification of safeguards risk.

WHY SAFEGUARDS RISK?

The definition of safeguards risk we use here is a combination of the potential threat, facility vulnerability to various malevolent events that may be attempted by the various adversary groups, and the consequences that may occur if the malevolent event is sucessfully carried out. The specific combination rule is not extremely important nor is the particular value assigned to the risk for a given event at a given facility. For inspection scheduling and other uses, the relative ranking among facilities is important. For reactor safety, probabilistic risk analysis uses a multiplicative rule where the probability of an event occurring is multiplied by a quantitative estimate of the consequences of the event to arrive at the overall risk. Here, we will describe a similar multiplicative rule where we multiply the threat, vulnerability, and consequence rankings to obtain a relative risk ranking.

Relative risk is seen as a systematic and more appropriate measure for inspection scheduling than by consideration of only one element of risk, for example, vulnerability. Even in the design or upgrading of security systems, one should not be driven by vulnerabilities (or threats or consequences) alone. An example of a threat driven response was the short-lived sky-marshalls of the airplane hijacking era. In this example, there were dozens

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, makes 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.

of hijackings each year in the U.S. representing an actual, not potential, threat. The early response to this threat was the sky-marshall approach which was later replaced by a more conventional approach of establishing a protected area around the aircraft, access controls for employees, and pre-board weapons screening for passengers.

Being consequence driven also has pitfalls. The actual consequences of the Three Mile Island accident were not serious; however, the public perception, fed by the media, was one of grave danger. This led to the requirement for state and local participation in emergency planning at all licensed power reactors. The emergency planning zone was arbitrarily set at a radius of ten miles. The result has been that several completed reactors appear to remain hostage to antinuclear political pressure groups.

A common example of vulnerability driven responses occurs following each DOE inspection where unsatisfactory ratings are found. It is clear that not every potential vulnerability must be corrected at once since it may be that the consequences associated with that vulnerability are minimal. Consideration of these examples has provided the impetus for exploring a safeguards risk approach where each element, threat, vulnerability, and consequence, are considered in combination.

MALEVOLENT EVENTS AND FACILITIES

The inability to quantify the probability of a given threat has resulted in the approach we describe here. Basically we first consider the malevolent events which safeguards and security systems are expected to protect against. Then we list the various facility types we wish to schedule for inspection. Some examples are reactors (production and research), fuel fabrication plants,

and power administrations. Next we construct a set of feasible malevolent event/facility combinations or pairs. These event/facility pairs constitute a generic set of scenarios which may be ranked against the characteristics of a given set of threat groups. This first ranking of the event/facility pairs in regard to the characteristics of the various threat groups constitutes the threat ranking. An example of this first ranking will help illustrate the approach. First, we assume there are three malevolent events:

1. Theft of SNM
2. Radiological Sabotage
3. Industrial Sabotage

We will use the three facility types mentioned above: reactors, fuel fabrication plants, and power administrations. Note immediately that some events are impossible or not feasible at some facility types; for example, theft of SNM is not possible at a power administration. Hence our example might yield the following feasible event/facility pairs:

1. SNM theft at a reactor
2. Radiological sabotage at a reactor
3. Industrial sabotage at a reactor
4. SNM theft at a fuel fabrication plant
5. Radiological sabotage at a fabrication plant
6. Industrial sabotage at a fabrication plant
7. Industrial sabotage at a power administration facility

These seven event/facility pairs constitute the totality of feasible event/facility scenarios. Now for simplicity, we may assume that there are only two threat groups; terrorists and economically motivated criminals. The

motivations, knowledge, capabilities, and numbers of these two threat groups may be analyzed in regard to the seven event/facility pairs. Clearly one may now rank the event/facility pairs by adversary group from the more likely to the less likely. Here one must consider the motivations and capabilities of these groups. One may assign, for example, a rank of "1" for the most likely, a "2" for somewhat less likely, and a "3" for the least likely event/facility pair for each of the threat groups. This would now give a total of fourteen event/facility/threat group combinations. Further analysis may reduce this to a smaller "most" likely set of combinations. Hence, we have obtained the "threat" ranking of the set of event/facility pairs.

VULNERABILITY RANKING

The result of the previous section yields a ranking of the event/facility pairs for a spectrum of threat groups. These results essentially constitute a set of generic scenarios which may be analyzed qualitatively or quantitatively by any one of several methods. Depending on the event and facility in question, one may apply vulnerability assessment models that have been developed by DOE contractors over the last 5-10 years. A qualitative approach may entail consideration of the portability of the material (for the case of SNM theft), the defense posture of the facility, and the effectiveness of barriers. Because of the extensive work done in this area, the ranking of the event/facility pairs in order of decreasing vulnerability should be easily accomplished. For example, using the ranking range of the previous section, a "1" may be assigned for a highly vulnerable event/facility pair; a "2" for somewhat less vulnerable, and a "3" for the least vulnerable event/facility

pair. Again, the absolute value is not important; it is only necessary to get the pairs in the correct "relative" order.

CONSEQUENCE RANKING

The consequences of a malevolent event may be characterized with regard to several elements. First, would be the health and safety of workers and the general public. Such impacts might arise if SNM was stolen and then used in a crude nuclear weapon or from radiological sabotage of a reactor. Of concern also would be national security impacts resulting from a loss of program continuity from a successful industrial sabotage act. As is the case with vulnerability ranking, a number of analytical tools may be utilized to obtain a consequence ranking of each event/facility pair. For radiological sabotage, one may use the CRAC Code (Calculation of Reactor Accident Consequences) or modifications (CRAC2, NUCRAC, etc.). Other, simpler calculations may also be used to obtain health and safety estimates. Some of the steps used to estimate health and safety impacts are however imprecise, such as the characterization of the source term, release fraction, and plume height. However, if a consistent approach is used for each event/facility pair, a "relative" ranking of consequences should be possible. Here again, we may assign a "1" as the most severe consequence, with a "3" as the least serious consequence rank.

RELATIVE RISK AND INSPECTION SCHEDULING

The relative risk may now be computed for each event/facility pair as simply the product of each of the three rankings; the threat ranking, vulnerability ranking, and the consequence ranking. From the simple example above, a pair representing a relatively high risk would have a ranking of 1,

the least risk ranking would be 27. Inspection scheduling could now be approached using the resulting relative risk ranking for all the event/facility pairs of interest. For example, all event/facility pairs having a relative risk ranking of 1 or 2 would mean that these pairs have at least two of the risk elements ranked at the top. These facilities might be inspected on a very frequent basis. Those pairs where the relative ranking is less than or equal to 8 might be scheduled for inspection on a less frequent basis. Under constrained inspection resources this approach has several advantages. Clearly it is rational and systematic. It is also self correcting in that as upgrades are completed at a facility to reduce vulnerability, that facility will rank lower in the overall risk ranking and hence will be inspected less frequently. Further refinements in computing the relative risk ranking may be tried; for example, a weighted system where one of the elements (say the vulnerability) is more heavily weighted than the others. However, one must be sure to maintain a balanced consideration of each element in order to arrive at a relative risk ranking.

lim