UCRL--94162

DE86 012816

THE SAFEGUARDS EVALUATION METHOD FOR EVALUATING VULNERABILITY TO INSIDER THREATS

Rokaya A. Al-Ayat
Bruce R. Judd
Therese A. Renis

This paper was prepared for submittal to
INMM 27th Annual Meeting
New Orleans, Louisiana
June 22-25, 1986

Lawrence Livermore National Laboratory

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

THE SAFEGUARDS EVALUATION METHOD FOR EVALUATING VULNERABILITY TO INSIDER THREATS

Rokaya A. Al-Ayat, Bruce R. Judd, and Therese A. Renis

Lawrence Livermore National Laboratory*

Livermore, California

Abstract

As protection of DOE facilities against outsiders increases to acceptable levels, attention is shifting toward achieving comparable protection against insiders. Since threats and protection measures for insiders are substantially different from those for outsiders, new perspectives and approaches are needed. One such approach is the Safeguards Evaluation Method. This method helps in assessing safeguards vulnerabilities to theft or diversion of special nuclear material (SNM) by insiders. The Safeguards Evaluation Method--Insider Threat is a simple model that can be used by safeguards and security planners to evaluate safeguards and proposed upgrades at their own facilities. The method is used to evaluate the effectiveness of safeguards in both timely detection (in time to prevent theft) and late detection (after-the-fact). The method considers the various types of potential insider adversaries working alone or in collusion with other insiders. The approach can be used for a wide variety of facilities with various quantities and forms of SNM. An Evaluation Workbook provides documentation of the baseline assessment; this simplifies subsequent on-site appraisals. Quantitative evaluation is facilitated by an accompanying computer program. The method significantly increases an evaluation team's on-site analytical capabilities, thereby producing a more thorough and accurate safeguards evaluation.

Introduction

In response to repeated international acts of terrorism directed against the United States, the U.S. government has given high priority to increasing security against external threats. For example, highly visible physical protection measures have been implemented at DOE facilities that handle special nuclear material (SNM) or nuclear components.

Only recently has attention shifted from external to insider threats. As protection against outsiders is increased to acceptable levels, safeguards and security activities shift toward achieving balanced protection against both outsiders and insiders. However, since the nature of the threats and protection measures is substantially different for insiders, as contrasted with outsiders, new perspectives and approaches have been adopted to assess safeguards effectiveness against insider threats. For example, insiders have routine access to SNM, knowledge of safeguards and operations, the flexibility to choose the ideal conditions for a theft attempt, and possibly the means by which to cover up the theft, at least temporarily. Also, since most insiders have authorized access to SNM, many of the protection measures against SNM theft are procedural rather than hardware-oriented (as is the case for outsiders).

Many of the early approaches developed to evaluate the vulnerability to insider theft or diversion of SNM are complex models that require time-consuming analyses. Consequently, those models have been of little use to safeguards and security planners with limited time and resources. The Safeguards Evaluation Method--Insider Threat is a relatively simple model based on the more complex models. It was developed by Lawrence Livermore National Laboratory specifically for safeguards and security planners to use in evaluating the safeguards at their own facilities. Also, the LLNL method is transportable so that it can be used by appraisal teams as they visit various facilities in the field. The method has been applied successfully at several DOE facilities to assess, in short periods of time, the vulnerability of safeguards systems to insider threats.

An Evaluation Workbook and computer software were developed to facilitate use of the Safeguards Evaluation Method. The workbook was developed to guide an evaluation team through the systematic steps of the method. The workbook serves as a means of documenting the characteristics of the facility and safeguards, and of noting the assumptions made during an evaluation.

Quantitative evaluation is facilitated by an accompanying computer program, the Safeguards

*Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Evaluation Tool (ET). This computer program's analytical tasks include safeguards evaluation, sensitivity analysis, and documentation. The computer-aided evaluation provides finer resolution of strengths and weaknesses and allows the user to quantify the benefits of safeguards improvements. Coupled with the workbook, the computer program can be used by facility operators for self-evaluation and for testing the effectiveness of safeguards modifications before implementation. A separate computer program combines ET results with cost information to evaluate the cost-effectiveness of various safeguards upgrade options.

The Safeguards Evaluation Method evaluates the effectiveness of an integrated system of physical security and material control and accountability against the insider threat. In particular, the method allows an evaluation team to assess a safeguards system's effectiveness in both timely and late detection of a theft or diversion of SNM. Detection is timely if a theft attempt is discovered before the material leaves the site boundary. Late detection occurs if material is discovered missing after it has left the site.

For timely detection, the method divides a theft attempt into three stages: SNM acquisition, removal from the Material Access Area (MAA), and removal from the Protected Area (PA). A theft attempt is considered successful when an adversary accomplishes all three stages. The method defines diversion of SNM as the removal of SNM from its authorized location (but not necessarily from the site), and this is considered the same as the acquisition stage of SNM theft.

Late detection, which occurs after-the-fact, is also important because it provides an indication that SNM may be missing. The sooner a material loss is detected, the greater the possibility of mitigating the consequences. An analyst can use the Safeguards Evaluation Method to assess (1) the probability that safeguards detect missing SNM and (2) the time lapse before detection.

The method is structured to consider all potential insider adversaries and their choices of possible strategies at each stage of a theft attempt. The method assumes that an adversary will choose the strategy at each stage of a theft attempt that gives him or her the lowest chance of detection. Once the analyst assesses the probability of detection for each adversary using each strategy, the method calculates the overall probability of timely detection for each adversary. Results can be aggregated over all potential adversaries by weighting the adversaries by their relative threat likelihood. These detection probabilities are used to identify safeguards' strengths and weaknesses, and they also indicate, when probabilities of detection are too low, where corrective actions are needed.

The method can be used to assess safeguards strengths and weaknesses against adversaries either working alone or in collusion with other insiders. To identify major safeguards weaknesses, the method can be applied initially to evaluate safeguards against single employees. If the safeguards system performs well against single employees, the analysis can be expanded to include collusion of two or more insiders.

The Safeguards Evaluation Method can be used at various levels of detail. It can be used qualitatively to give the evaluation team a general idea of the main strengths and weaknesses of safeguards. The accompanying ET computer program can be used for quantitative analysis to compare safeguards performance against various adversaries and strategies. The results provide a basis from which to make upgrade recommendations. The method can then be used to evaluate the potential improvement in effectiveness (i.e., the benefit) that could be achieved by the recommended upgrade alternatives.

The method provides a systematic and practical approach to safeguards evaluation. The approach can be used for a wide variety of facilities with various quantities and forms of SNM. In each case, the analysis is tailored to the types of threats that are important at a particular facility. The method is being expanded to consider other threats such as sabotage, espionage, and computer security.

The Safeguards Evaluation Method requires an evaluation team, composed of specialists in physical security, material control and accountability, and operations. The method is implemented in three steps: the plant tour; documentation of the facility layout, threats, and safeguards in the Evaluation Workbook; and evaluation of safeguards effectiveness. These steps are described below.

Plant Tour

The purpose of the plant tour is to understand the layout and functions of the facility to be evaluated; the quantities, forms, and locations of SNM in the facility; who has access to SNM; paths for removing SNM from the material access area and protected area; and the various safeguards components.

Although information about the facility, material, procedures, operations, personnel access, and material control and accountability can often be found in facility documentation, the plant tour is essential. The plant tour allows the evaluation team to observe and understand how procedures are implemented in practice. If procedures aren't followed exactly as prescribed, credit should be given only to their effectiveness in practice.

Information on how safeguards oparate in practice is gained through interviews with facility personnel responsible for plant operations, security, material control, and material accountability.

Evaluation Workbook

The Evaluation Workbook provides a means of documenting the facility safeguards and the assumptions made in evaluating the vulnerability to insider threat. The workbook guides the evaluation team in asking the appropriate questions to gather information for the evaluation.

Threats and safeguards are noted in the workbook. Threat descriptions include a list of the various potential adversaries and their authority, access to SNM, and the number of each adversary type allowed within the facility.

Table 1. Qualitative evaluation.

No.	Adversary	Stages/Strategies/Qualitative Effectiveness						
		SNM Removal		MAA Removal			PA Removal	
		Can	Glove	Disable	Evac	Alarm	Walk	Throw
1	Operator	High	[✓ Low]	High	[✓ Low]	High	[✓ Low]	[✓ Low]
2	Custodian	[✓ Med]	High	[✓ Low]	Med	[✓ Low]	[✓ Low]	[✓ Low]

Safeguards components, especially those designed to limit access to SNM or detect its unauthorized movement, are recorded. Safeguards designed to protect against insider threat, such as the two-person rule, are often procedural rather than hardware-oriented. Thus, it is important to observe safeguards hardware components and understand how procedures are implemented.

Analysis of Timely Detection

After collecting and documenting information about the facility, its threats, and safeguards, the evaluation team uses this information to describe the various strategies an adversary could use at each stage of SNM theft. Recall, the three stages of SNM theft are SNM acquisition, MAA removal, and PA removal.

SNM acquisition includes the acts of gaining possession of SNM inside the MAA and concealing the SNM in an unauthorized location for later removal. MAA removal includes transporting SNM from inside the MAA to a location outside the MAA and concealing the material in the Protected Area (PA) for later removal. Finally, PA removal means taking the SNM off site.

In developing each strategy, we assume that an adversary uses stealth and deceit and chooses conditions that minimize detection likelihood. Some of the considerations an adversary takes into account are:

- Timing of the attempt.
- Exploiting special knowledge, access, or authority.
- Including actions to:
  - defeat safeguards by tampering or deceit, and
  - delay detection by falsification of records or substitution of material without increasing the adversary's risk.

These strategies and the safeguards in place that may prevent or detect them are documented in the Evaluation Workbook. If different adversaries have different means of carrying out a strategy, the differences are noted.

Qualitative Evaluation

Qualitative evaluation allows an analyst to make general statements about the effectiveness of safeguards against each adversary and at each stage of a theft attempt. The analyst describes safeguards effectiveness with adjectives such as high, medium, or low.

Table 1 shows how qualitative assessments can be made by rating the safeguards effectiveness against each adversary using each strategy. At each stage of a theft attempt, the assessments are used to determine an adversary's best strategy. Recall, the method assumes that at each stage of a theft attempt, an adversary will choose the strategy that affords him or her the lowest probability of timely detection. For example, if an adversary has two possible strategies for acquiring SNM--one with high safeguards effectiveness and one against which safeguards have a medium effectiveness--the adversary will minimize his or her chances of being detected by choosing the strategy against which safeguards have only medium effectiveness. The Evaluation Workbook contains forms that facilitate this type of qualitative evaluation.

Table 1 shows the strategies each adversary would choose at each stage of a theft attempt. The qualitative judgments allow the evaluation team to make statements about overall safeguards effectiveness in preventing a successful attempt of SNM theft and in comparing the effectiveness of safeguards against adversaries at each stage of a theft attempt. However, it is not clear how the qualitative judgments could be combined to compare the effectiveness of safeguards against different adversaries.

Quantitative Evaluation

It is often necessary to make comparisons among adversaries in deciding how to allocate limited resources for safeguards upgrades. Making quantitative judgments of effectiveness facilitates such comparisons among adversaries, strategies, stages of a theft attempt, and safeguards upgrades. The probability of timely detection is the quantitative measure of effectiveness used in the Safeguards Evaluation Method.

Table 2 below shows an illustrative quantitative assessment. The ET computer program can be used to combine the safeguards effectiveness at each stage to calculate the overall probability of timely detection for each adversary.

As illustrated in Fig. 1, the overall probability of timely detection of each adversary is one minus the probability that the adversary successfully completes all stages of a theft attempt

Table 2. Quantitative evaluation.

No.	Adversary	Timely Detection Probabilities for Theft Strategies								
		SNM Removal		MAA Removal			PA Removal		Computed	
		Can	Glove	Disable	Evac	Alarm	Walk	Throw	Prob	Weight
1	Operator	0.80	0.20	0.90	0.20	0.80	0.10	0.20	0.42	10
2	Custodian	0.60	0.80	0.20	0.60	0.20	0.10	0.20	0.71	2
	WEIGHTED AVERAGE	0.77	0.30	0.78	0.27	0.70	0.10	0.20	0.47	12

when he uses his or her "best" strategy at each stage. In other words:

$$\text{Prob}\left\{\begin{matrix}\text{timely}\\ \text{detection}\end{matrix}\right\} = 1 - \left[\text{Prob}\left\{\begin{matrix}\text{no detection}\\ \text{during SNM}\\ \text{acquisition}\end{matrix}\right\} \times \text{Prob}\left\{\begin{matrix}\text{no detection}\\ \text{during MAA}\\ \text{removal}\end{matrix}\right\} \times \text{Prob}\left\{\begin{matrix}\text{no detection}\\ \text{during PA}\\ \text{removal}\end{matrix}\right\}\right] .$$

Aggregated--or weighted average--results for all adversaries can be calculated by assigning weights to the different types of potential adversaries. Weights can be assigned based on the relative numbers of each adversary type that have access to the facility, or by some other scheme such as the relative amount of time that various adversaries have access to areas where SNM is located. The aggregated results can be used for comparisons of safeguards effectiveness for proposed upgrades relative to the effectiveness of current safeguards.

Late Detection

If safeguards fail to detect theft of SNM in time to prevent the theft, it is important that the safeguards eventually detect that SNM is missing. The longer it takes to detect missing SNM, the more difficult it is to determine what happened to the material. The Safeguards Evaluation Method provides a means for assessing the probability of late detection and the median time to detection.

To assess the safeguards effectiveness in late detection, it is first necessary to identify the events that could detect that SNM is missing. Late detection events are usually material accountability procedures or processing requirements. For example, if SNM is requested from the vault for processing and is missing, its absence will be detected. Similarly, missing material may be discovered during a periodic inventory.

Many of the late detection events are periodic. It is possible that if the first occurrence of a late detection event does not detect missing SNM, a subsequent occurrence of the event may provide detection. The Safeguards Evaluation Method allows the evaluation team to define a late detection event and, if appropriate, its period of recurrence. The team then assesses the probability of detection for the first occurrence of the event and for the second occurrence of the event. Based on effectiveness assessments for the first two occurrences of a late detection event, the ET computer program fits a Weibull distribution to these two occurrences to estimate safeguards effectiveness of the subsequent occurrences of the event. Figure 2 is an example of how the cumulative probability of detection approaches 1.0 when modeled with the Weibull distribution.

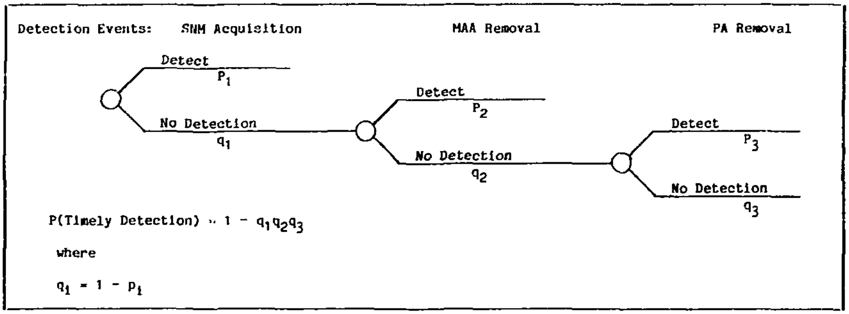

Fig. 1. Calculating the probability of timely detection.

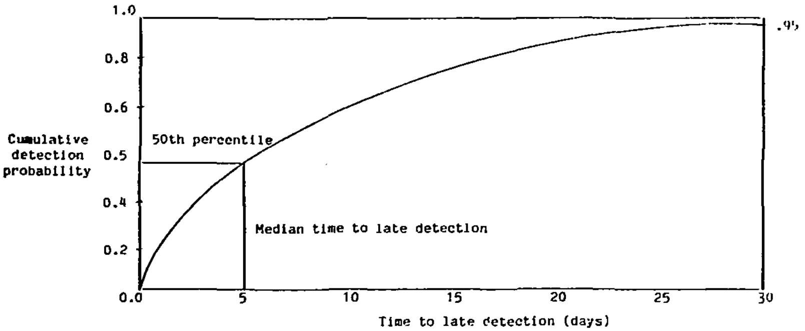

Fig. 2. Probability of late detection vs. time to late detection

The ET computer program calculates the probability of late detection in a manner similar to the way it calculates the probability of timely detection. The calculation is based on all late detection events. ET also calculates the median time to late detection. The median time to late detection of a hypothetical adversary is the time at which there is a .5 probability of having already detected that SNM is missing and, therefore, a .5 probability that it will take longer than the median time to detect missing SNM. Figure 2 shows a 5-day median time to late detection for a hypothetical adversary.

Sensitivity Analysis

Since the effectiveness of safeguards in both timely and late detection of SNM theft is assessed subjectively, there is often debate over the accuracy of assessments. Thus, it is necessary to test the sensitivity of the results to the particular assumptions and assessments made during an evaluation. The ET computer program gives the evaluator a simple means for determining the effect of changing assumptions and assessments. The results from changing an assumption can be compared with base-case results to assess the effect of the assumption. Sensitivity analysis highlights the sensitive inputs that require closer investigation and focuses debate on the most important issues.

Evaluating Safeguards Upgrades

As an extension of sensitivity analysis, the Safeguards Evaluation Method can be used to evaluate the effectiveness of proposed safeguards upgrades. To evaluate the change, the evaluation team can change the safeguards effectiveness assessments for those strategies that would be affected by the proposed safeguards upgrades.

Using separate software, the team combines estimates of the incremental cost of each upgrade and the relative changes in safeguards effectiveness due to that upgrade; this produces a cost/benefit analysis of the proposed upgrades. As the cost of successive upgrades increases, additional safeguards effectiveness per unit cost may reach a point where additional upgrades are not cost-effective. At that point, a decision-maker may decide to accept the remaining risk rather than implement additional upgrades.

Conclusion

Six three-day workshops were conducted in 1985 and 1986 to train safeguards and security planners to apply the Safeguards Evaluation Method--Insider Threat at their own facilities. The workshops include lectures, example evaluation exercises, and hands-on use of the computer program. After attending the workshop, several participants have applied the method at a number of DOE facilities.

The Safeguards Evaluation Method is being used by DOE operations offices and contractors to evaluate vulnerabilities to insider threats. The results will be used in developing their Master Safeguards and Security Agreements with DOE. Concurrently, the method is being presented to representatives of the various DOE facilities as part of the 12-day Tactical Vulnerability Assessment Training Program at the DOE Central Training Academy in Albuquerque. Four sessions of the Training Program with 50 participants in each have been scheduled for June, 1986 through December, 1986.

When first applied to a facility, the Safeguards Evaluation Method may take a full week in order to provide a thorough analysis and documentation of facility operations and safeguards effectiveness. However, the first application provides an important baseline assessment, which simplifies subsequent on-site appraisals. The method significantly increases the evaluation team's on-site analytical capabilities, thereby producing a more thorough and accurate safeguards evaluation for the same level of effort. Experience with the method increases awareness of insider threats and thereby improves the design of new safeguards.