UCRL--96932

DE87 013485

Tactical Vulnerability Assessment Training Program

R. A. Al-Ayat, B. R. Judd, T. A. Renis
Lawrence Livermore National Laboratory

W. K. Paulus, A. E. Winblad
Sandia National Laboratory

B. R. Graves
Central Training Academy

This paper was prepared for submittal to
INMM 28th Annual Meeting
Newport Beach, California
July 12-15, 1987

July 10, 1987

Lawrence Livermore National Laboratory

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California 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 products, 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 the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

Tactical Vulnerability Assessment Training Program

R. A. Al-Ayat, B. R. Judd, T. A. Renis,
Lawrence Livermore National Laboratory[*]

W. K. Paulus, A. E. Winblad
Sandia National Laboratory

B. R. Graves
Central Training Academy

Abstract

The Department of Energy sponsors a 9-day training program for individuals who are responsible for evaluating and planning safeguards systems and for preparing DOE Master and Security Agreements (MSSAs). These agreements between DOE headquarters and operations offices establish required levels of protection. The curriculum includes: (1) the nature of potential insider and outsider threats involving theft or diversion of special nuclear material, (2) use of computerized tools for evaluating the effectiveness of physical protection and material control and accountability systems, and (3) methods for analyzing the benefits and costs of safeguards improvements and for setting priorities among proposed upgrades. The training program is varied and highly interactive. Presentations are intermixed with class discussions and "hands-on" analysis using computer tools. At the end of the program, participants demonstrate what they have learned in a two-and-one-half day "field exercise," which is conducted on a facility scale-model. The training program has been conducted six times and has been attended by representatives of all DOE facilities. Additional sessions are planned at four-month intervals. This paper describes the training program, use of the tools in preparing MSSAs for various DOE sites, and recent extensions and refinements of the evaluation tools.

Introduction

The Department of Energy (DOE) sponsors a 9-day training program for individuals responsible for planning safeguards systems and evaluating their effectiveness at facilities handling special nuclear material (SNM). The training program is also designed for personnel responsible for preparing or providing input for their site's Master Safeguards and Security Agreements (MSSAs). These agreements between DOE headquarters and operations offices establish required levels of protection.

In 1985 the DOE Office of Safeguards and Security (OSS) recognized the need for a training program presenting standardized tools for identifying vulnerabilities and conducting cost-benefit analyses of suggested improvements. Accordingly, in November, 1985, the Integrated Vulnerability Assessment Committee was formed with members from Lawrence Livermore, Sandia, and Los Alamos National Laboratories, and representatives from DOE Headquarters and contractors. The Committee's goals were:

- o Develop computerized evaluation tools for identifying vulnerabilities to both the insider and outsider threats. The tools must run on a personal computer, and their use must be easily teachable to DOE safeguards and security specialists. Moreover, these tools should be capable of supporting the DOE facilities' planning process; i.e., the tools must provide the supporting rational for developing MSSAs, site plans, and five-year plans.
- o Design a curriculum to train representatives from all DOE operations offices and their contractors. Again, the training curriculum must be consistent with the needs of a variety of DOE personnel, which includes: security specialists, safeguards analysts, material control and accountability personnel, and facility operations personnel.
- o Offer the training program at the DOE Central Training Academy in Albuquerque, as needed. The first workshop was held in June, 1986, and five workshops were offered subsequently.

Contents of the Training Program

Participants in the TVATP learn to use three analytical tools: ET for evaluating protection against the insider threat; SAVI for the outsider threat; and MI$ER, a method developed to integrate ET and SAVI results. MI$ER also allows comparison of benefits from various upgrade packages, and the program identifies those upgrades that achieve the greatest benefit in protection at a given cost.

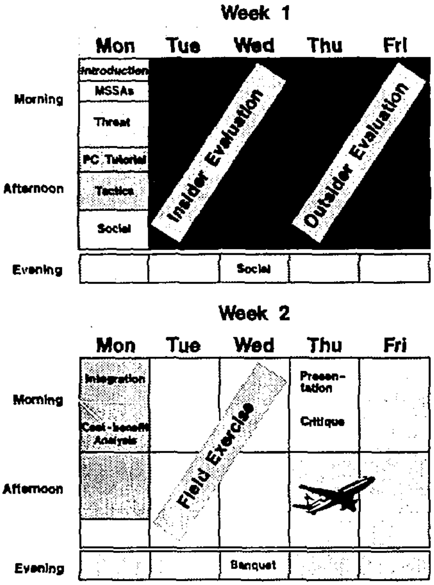
This paper describes the schedule and content of the training program and provides a discussion of our experience teaching the workshops. It also

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

describes the philosophy on which the methods are based and discusses in detail the schedule for teaching the three tools. The paper concludes with a brief discussion of future directions for the training program and planned enhancements to both ET and SAVI.

Workshop Schedule

The training program spans nine days. Figure 1 provides details of the schedule. The first day is devoted to discussion of the threats and adversary tactics. Next, participants are instructed on ET and SAVI. Each tool requires a two-day learning period. The second week begins with one day of training on the use of MI$ER. This is followed by a two-and-one-half-day field exercise. The field exercise provides the attendees an opportunity to demonstrate proper use of the vulnerability assessment tools on a scale-model facility. The results of the scale-model evaluations are then presented by the students to all workshop attendees and instructors. The presentations are discussed and critiqued by participants and faculty members from Livermore and Sandia National Laboratories.



Week 1

	Mon	Tue	Wed	Thu	Fri
Morning	Introduction MSSAs Threat	Insider Evaluation		Outsider Evaluation	
Afternoon	PC Tutorial Tactics Social				
Evening			Social		

Week 2

	Mon	Tue	Wed	Thu	Fri
Morning	Integration Cost-benefit Analysis	Field Exercise		Presentation Critique	
Afternoon					
Evening			Banquet		

Fig. 1. TVATP training schedule.

Insider Evaluation Method (ET)

The Safeguards Evaluation Method for Insider Threat (ET) aids in evaluating the effectiveness of physical security and material control and accountability systems against theft of SNM by nonviolent insiders. ET is a simple tool that can be used by safeguards and security planners to evaluate existing safeguards and proposed upgrades at their own facilities. The method considers nonviolent insiders acting alone or in collusion with other insiders, and it can be used to evaluate the effectiveness of safeguards in both timely (in time to prevent theft) and late (after-the-fact) detection. The approach applies to a wide variety of facilities with various quantities and forms of SNM. The method includes a workbook and the ET computer software.

The objectives of the insider threat evaluation (ET) portion of TVATP are to give participants a clear understanding of:

- o The nature of potential insider threats to SNM at DOE facilities.
- o Current insider protection methods, human reliability programs, physical security measures, material control procedures, and material accountability systems.
- o Practical techniques for identifying needed improvements and designing effective upgrades.

Each student is given a copy of the Insider Safeguards Evaluation workbook. The workbook guides the analyst through an evaluation. The workbook contains forms that, when completed, document the facility safeguards and the assumptions made during the evaluation. Each student is also given a copy of the accompanying ET computer software.

The format of ET instruction is highly interactive. Four different instruction modes are employed: classroom presentations, a practical exercise, small group sessions, and "hands-on" analysis with microcomputers. The classroom presentations are informal, with ample time devoted to discussions among the participants. These discussions allow participants to exchange concerns, problems, and solutions among people working with different functional areas and facilities. The discussions also foster an acceptance of the concepts and methods presented.

The concepts and techniques presented in the classroom are demonstrated in a comprehensive practical exercise. This exercise involves the evaluation of safeguards at a fictitious nuclear material processing facility. Participants "tour" the facility by watching slides and listening to a description of the physical layout, operating procedures, and safeguards implemented at the facility. Students then document safeguards and evaluate the safeguards' effectiveness. During most of the exercise, the participants work in small groups of three to five people. The groups are composed of members from different facilities and are arranged to reflect the mix of skills used in a typical evaluation, which includes personnel representing operations, physical security, and material control and accountability.

Computers are used throughout the evaluation exercise. Each small working group is provided with a computer to evaluate safeguards by using the ET computer program. In addition to their own computer, each group has a second monitor which is connected to the instructor's computer. This makes it possible for all participants to follow the instructor's use of the program on the "slave" monitors, while at the same time utilizing the program on their own computers.

Analysis using ET begins by documenting the safeguards in the example facility and defining the adversary types. Potential insider adversaries include any employee with access to SNM. The workshop students model theft of SNM by dividing a theft attempt into three stages: SNM acquisition, removal from the material access area (MAA removal), and protected area (PA) removal. Timely detection occurs when a theft attempt is detected before the material leaves the PA boundary. Participants learn to evaluate the timely detection capabilities of safeguards by identifying insider strategies at each stage of theft and then assessing the probability of detection for each type of insider using each strategy.

To evaluate the late detection capabilities of safeguards, students identify late detection events such as material control and accountability procedures and SNM processing requirements. The students then assess the probability that each late detection event will discover SNM is missing. ET uses this information to compute the probability and time to late detection. ET provides the user with tabular and graphical results. Figure 2 shows a bar graph displaying the probability of timely detection against the spectrum of insider adversaries. The figure highlights the strengths and weaknesses in the system.

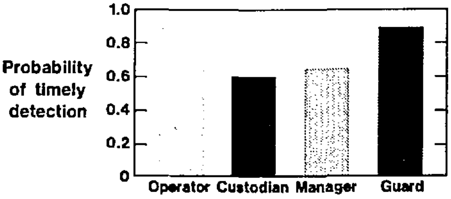


Fig. 2. Safeguards effectiveness against a spectrum of insider adversaries.

Once the evaluation of the effectiveness of existing safeguards is complete, students learn how to analyze the sensitivity of their results to underlying assumptions: e.g., the effectiveness of individual safeguards components and procedures and the adversary's capabilities.

Participants analyze evaluation results and identify the vulnerabilities of existing safeguards and paths to particular adversaries and strategies. Based on the vulnerabilities identified, upgrades are suggested and grouped into "packages." The impact of each package on safeguards effectiveness is then evaluated.

Other issues in evaluating safeguards against the insider threat are discussed briefly. These issues include: evaluating safeguards at multiple targets or buildings at a facility; and evaluating the effectiveness of safeguards against additional threats (such as violent insiders, two insiders in collusion, and insider-outsider collusion).

Outsider Evaluation Method (SAVI)

The SAVI software package is used to model and assess the vulnerability of a facility to specified outsider threats. SAVI is a PC-based path-analysis model that evaluates the physical protection system by calculating the probability of interruption, P(I), of the adversaries by the response force before the adversaries complete their mission. SAVI can analyze sabotage and theft attacks in which adversaries are interrupted at the target, as well as theft attacks in which adversaries are contained within the site boundary. The output of SAVI is a ranking of the ten most vulnerable paths in a facility in order of the P(I). Figure 3 shows typical SAVI output illustrating the P(I) and corresponding time remaining after interruption (TRI) for a given response force time (RFT).

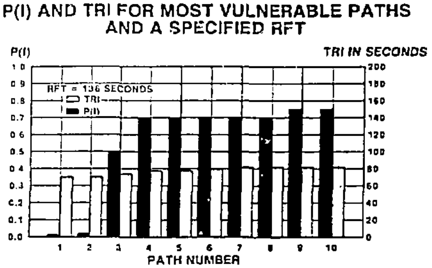


Fig. 3. Vulnerable path analysis results produced by SAVI

The use of SAVI is taught in six sessions: (1) Physical Protection System Concepts, (2) SAVI Modeling, (3) SAVI Software, (4) Protection Component Lists, (5) Practice Example Facility, and (6) Upgrades Analysis. A brief description of these sessions follows.

Physical Protection System (PPS) Concepts

The first session is a description of the way the three basic functions of the PPS -- detection, delay, and response--are integrated in SAVI using a path-event time line. Factors that must be considered in estimating the response force time to be used in the P(I) calculation are reviewed, and the concept is introduced of a critical detection point (CDP) on a path. The CDP is identified as the "last chance" point for detection if the response force is to arrive in time to interrupt the adversaries.

SAVI Modeling

In this session the concept of a generic adversary sequence diagram, ASD, is introduced. Figure 4 shows the generic adversary sequence diagram used by SAVI. The ASD models physical areas--separated by layers of protection elements--to represent a facility and its PPS. A demonstration is given of the construction of a site-specific ASD from the generic ASD by selecting the appropriate protection elements. Also used to model a specific facility are "jump operators" to cross protection layers and "bypass operators" to remove unwanted areas.

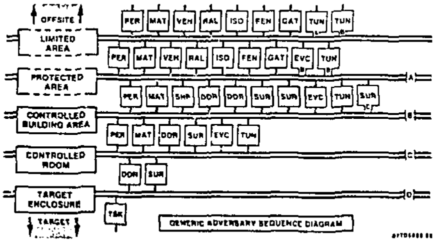


Fig. 4. Generic adversary sequence diagram

SAVI Software

The SAVI software session gives the students hands-on experience with the PC and the SAVI program. The SAVI menu structure is described and the students are led through the major submenus: FILE, MODIFY, THREAT, DEFINE, and ANALYZE. Next, participants step through an example in the SAVI Users' Manual to obtain experience in using the software.

Protection Components Lists

Each protection element is composed of generic detection-and-delay components. Lists are provided that contain these components, together with reference delay-times and detection probabilities based on field performance tests and expert judgments. In this session the students are shown the configuration of the components on each element and learn how to select the components for a specific facility, either from the reference lists or by setting their own values.

Practice Example Facility

In this session the students are given the description of a hypothetical facility consisting of site- and building-layouts and a written description of construction features, operations, target characteristics, security inspector and response force capabilities and deployments; and protection system specifications. The students then model the PPS for this facility, input the necessary data to SAVI, and analyze the vulnerability. At various stages in the process, each group of students presents their approach, and lively class discussions ensue.

Upgrade Analysis

This session presents an approach to analyze sensitivity and suggest upgrades to the baseline PPS. Concepts such as balanced protection and protection-in-depth are reviewed, and the students implement these concepts by using SAVI to analyze the effects of selected upgrades and of variations in the component values.

Method for Integrating SAVI and ET Results (MI$ER)

The MI$ER program is designed to integrate results of insider and outsider safeguards evaluations, to display the effectiveness of existing or upgraded safeguards, and to prioritize and determine the cost-effectiveness of upgrades.

MI$ER is normally used as a companion to ET and SAVI. The MI$ER program can analyze insider and outsider data separately or in combination. MI$ER helps set priorities among safeguards upgrades based on their costs and effectiveness. When both insider and outsider adversaries are considered, the relative weight given to the insider threat vis-a-vis the outsider threat helps determine priorities among upgrades in order to achieve balanced protection. MI$ER can help analyze the sensitivity of upgrade priorities to these weights and determine whether or not they are critical to the choice among upgrades. This provides the user a systematic framework for explicit and consistent analysis of safeguards upgrades.

The MI$ER session of TVATP teaches participants how to integrate the results of multiple analyses--especially insider and outsider threat analyses--for a single facility.

During the ET and SAVI sessions of TVATP, vulnerabilities and potential safeguards upgrades packages are identified. Using MI$ER, participants in TVATP learn to prioritize potential upgrades based on their costs and relative benefits. As with the ET and SAVI instruction, the format of MI$ER instruction is highly interactive. The concepts of MI$ER are taught using classroom presentations and computer-code demonstrations. Participants remain in the same small groups they worked with during the ET and SAVI instruction. Using MI$ER, the groups continue to evaluate the fictitious facility and to analyze proposed upgrades against both the insider and outsider threats.

During the MI$ER session, participants retrieve and edit data from ET and SAVI safeguards' evaluations. To integrate the results of multiple evaluations, participants assign relative weights to each adversary and threat type. Next, they review the suggested upgrade packages and their effectiveness from the ET and SAVI sessions. Upgrades packages are combined and evaluated using both ET and SAVI. MI$ER uses the results and the estimates of upgrades' costs to determine the relative prioritization of the upgrades. Figure 5 is an example of a cost-benefit analysis graph generated by MI$ER.

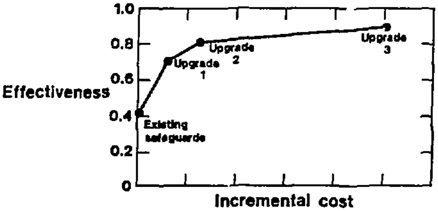


Fig. 5. Cost-benefit graph for prioritizing upgrades.

Field Exercise

At the end of the program, participants demonstrate what they have learned in a two-and-a-half-day "field exercise." The field exercise makes use of a scale-model of an example facility and written procedures describing the facility. Workshop participants are teamed with other safeguards analysts from their home facility to conduct a practice safeguards' evaluation.

At the beginning of the field exercise, safeguards and procedures at the facility are explained during a briefing and "tour" of the facility by instructors who impersonate personnel responsible for security, operations, and material control and accountability. The evaluation exercises are less formally structured than the previous sessions of the workshop. Evaluation teams document evaluation assumptions and features of the facility. More than one-half day each is dedicated to evaluating the insider and outsider threats. Timely- and late-detection capabilities against the insider are also evaluated. Vulnerabilities and potential upgrades for insider and outsider threats are identified and evaluated. Individual insider and outsider safeguards upgrades are "packaged" into low-, medium-, and high-cost options. The benefits of each upgrade package are evaluated using ET and SAVI. MI$ER is used to evaluate the cost and relative benefit of these upgrade packages and provide a priority ranking based on their costs and benefits.

At the end of the two-and-a-half-day field exercise, each team makes a 20-minute presentation of their evaluation results and recommendations. The presentations include descriptions of the scope of the analysis, insider and outsider effectiveness results, MSSA-required input data, safeguards strengths and weaknesses, potential upgrades, upgrades priorities, sensitivity analysis results, and a summary of the team's recommendations.

At the close of each workshop, participants provide feedback on strong and weak features of the workshop. Based on these critiques, the TVATP workshop has been refined continuously since it was first offered in June, 1986.

The training program has been conducted six times. Additional sessions are planned at four-month intervals. Use of the methods presented in TVATP has benefited the DOE community by enhancing the level of protection against potential insider and outsider threats, by making cost-effective use of safeguards resources in the short- and long-term, and by ensuring consistent and comprehensive safeguards and security policy.

Future Directions

The vulnerability assessment models presented during TVATP have been modified and improved since they were first released. The team assembled for developing TVATP continues to refine, expand, and develop vulnerability assessment models. Currently we are developing an integrated program for addressing both insider and outsider threats. The integrated program will be capable of evaluating safeguards effectiveness against a variety of threats: terrorists, criminals, demonstrators, single and colluding nonviolent insiders, and--to a limited extent--insiders in collusion with outsiders. The program will require a safeguards analyst to define a facility only once. The program will then be able to use that facility description for analysis of both the insider and outsider threats.

There will be many differences between the new insider model and ET: the new evaluation model will contain data bases of adversary attributes, strategies, and baseline probabilities of detection. In addition, probabilities of detection will depend upon the safeguards present and their implementation, as well as the access and authority of each insider adversary. The new outsider model will use a faster algorithm than SAVI and will model a larger spectrum of outsider adversaries. A model to calculate the probability of neutralization will be included.

The integrated package is due for release in early 1988, and it is expected that, after the release, a training program in the use of the package will be developed and offered at the DOE Central Training Academy.