LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR-88-1929

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--88-1929

DE88 014445

TITLE MODELING RISK ASSESSMENT FOR NUCLEAR PROCESSING PLANTS WITH LAVA

AUTHOR(S) S. T. Smith and R. M. Tisinger

SUBMITTED TO 29th Annual Meeting of the Institute of Nuclear Materials Management, Las Vegas, June 26-29, 1988

DISCLAIMER

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

MODELING RISK ASSESSMENT FOR NUCLEAR PROCESSING PLANTS WITH LAVA

Suzanne T. Smith and Richard M. Tisinger
Safeguards Systems Group, MS-E541
Los Alamos National Laboratory
Los Alamos, NM 87544

ABSTRACT

Using the Los Alamos Vulnerability and Risk Assessment (LAVA) methodology, we developed a model for assessing risks associated with nuclear processing plants. LAVA is a three-part systematic approach to risk assessment. The first part is the mathematical methodology; the second is the general personal computer-based software engine; and the third is the application itself. The methodology provides a framework for creating applications for the software engine to operate upon; all application-specific information is data. Using LAVA, we build knowledge-based expert systems to assess risks in applications systems comprising a subject system and a safeguards system. The subject system model is sets of threats, assets, and undesirable outcomes. The safeguards system model is sets of safeguards functions for protecting the assets from the threats by preventing or ameliorating the undesirable outcomes, sets of safeguards subfunctions whose performance determine whether the function is adequate and complete, and sets of issues, appearing as interactive questionnaires, whose measures (in both monetary and linguistic terms) define both the weaknesses in the safeguards system and the potential costs of an undesirable outcome occurring. LAVA applications include our popular computer security application and applications for embedded systems, survivability systems, transborder data flow systems, property control systems, and others.

INTRODUCTION

We used the Los Alamos Vulnerability and Risk Assessment (LAVA) methodology to develop a hierarchical structure and sets of fuzzy event trees for modeling risk assessment for nuclear safeguards systems. This structure is guiding our development of a complete automated LAVA applications system (LAVA/NSG) that assesses risks in nuclear safeguards systems.

LAVA/NSG addresses risks associated with such potential outcomes as theft or diversion of nuclear material, radiological sabotage, unauthorized control of nuclear weapons or test devices, and other concerns. LAVA/NSG is an alternative to existing quantitative methods, providing an approach that is both objective and subjective and producing results that are both quantitative and qualitative. In addition, LAVA/NSG can be used as a self-testing device in preparing for inspections, as a self-evaluating device in testing compliance with the various orders and criteria that exist, and as a certification device by an inspector or an inspection team.

LAVA is an original systematic approach to risk assessment developed at the Los Alamos National Laboratory to deal with risks inherent in massive, complicated systems.[1-5] Characteristics of such systems are huge bodies of imprecise data, indeterminate (and possibly undetected) events, large quantities of subjective information, and a dearth of objective information. The methodology has been used for our popular computer security application, LAVA/CS,[6] as well as applications for embedded systems, survivability systems, transborder data flow systems,[7] property control systems, and others.

THE LAVA SYSTEM

LAVA has three separate parts. The first part is the mathematics of the methodology—its mathematical underpinnings and technical basis. The second part is the general software engine, written for a widely used family of personal computers and structured to be independent of the applications that it drives. The third part is the application itself. The LAVA methodology provides a framework for creating applications for the general software engine to operate upon; all application-specific information is represented as data.

Using LAVA, we build knowledge-based expert systems for assessing risks in applications systems. There are two parts that define an application. The first part is the hierarchical structure and trees that define the model—the threat, asset, and outcome sets, the outcome possibility matrix, the safeguards functions for each threat-asset pair, based upon the kinds of interactions that might occur to result in one or more of the outcomes; the safeguards subfunctions for each function; mitigating factors for outcome severity

*Work supported by the U.S. Department of Energy, Office of Safeguards and Security.

and the contributing factors, both linguistic and monatary, to the potential cost of a successful atteck. The second part is the set of questionnaires, implemented as data sets for the general software engine to operate upon the vulnerability assessment questionnaire, the outcome severity mitigation questionnaire, the dynamic threat questionnaire (if applicable), and the monetary and linguistic impact (or cost) questionnaires.

The vulnerability assessment questionnaire for a given application is concatenated from a library of category questionnaires that come about from specific security orders, inspection criteria, interviews with various experts in the field, and general good security practice. The questions themselves represent individual safeguards (called "safeguards elements") or portions of safeguards (called "safeguards attributes") that are related through a database structure to one or several of the safeguards subfunctions. The vulnerability questionnaire can comprise from a few hundred to several thousand questions, depending on the required analytical depth.

The other questionnaires are all considerably smaller than the vulnerability questionnaire. The outcome severity mitigation questionnaire inquires about the presence and estimated effectiveness of any mitigating situations that might be pertinent. If intelligence information is available and analytical detail about the dynamic threat is required, the dynamic threat questionnaire seeks information about the motivation, capability, and opportunity of the current known threat and about the attractiveness of each asset set to the threat; if such information is not available, the user estimates a relative attractiveness factor for the asset sets and whether the dynamic threat is the same as or, in varying degrees, larger or smaller than the background (static) threat. The impact questionnaires ask cost-related questions in either linguistic or monetary terms. With the exception of the intelligence-based dynamic threat questionnaire, all of the questions in these questionnaires number in the single or double digits (usually not more than a dozen or so questions).

THE NUCLEAR SAFEGUARDS MODEL

For our nuclear safeguards model, LAVA/NSG, we postulate four assets: 1) nuclear material; 2) the facility, including physical plant and personnel; 3) machine interpretable information, including software, input and output files, and databases; and 4) human interpretable information, including documents, screen displays, graphs, charts, and so forth. The model's threat set consists of three threats: 1) natural, random, and environmental hazards; 2) onsite humans, including the authorized insider; and 3) offsite humans, such as terrorists and hostile intelligence agents. Figures 1-3 show the hierarchical structures for the three threat categories with respect to the four asset categories; included in these hierarchies, and discussed later in this paper, are the safeguards functions and subfunctions associated with each threat-asset pair.

There are seven undesirable outcomes considered in the current model: 1) theft; 2) diversion; 3) unauthorized control, use, or access; 4) radiological sabotage and radioactive release; 5) denial of use or loss of production capability; 6) damage or injury; and 7) unauthorized modification or disclosure. It is important to note that a single event can result in the simultaneous occurrence of more than one of the outcomes. Figure 4 shows the outcome possibility matrix for the threat-asset combinations; a value of zero indicates that the outcome is impossible for that threat-asset (T-A) combination, and a value of unity means the outcome is possible for that T-A pair.

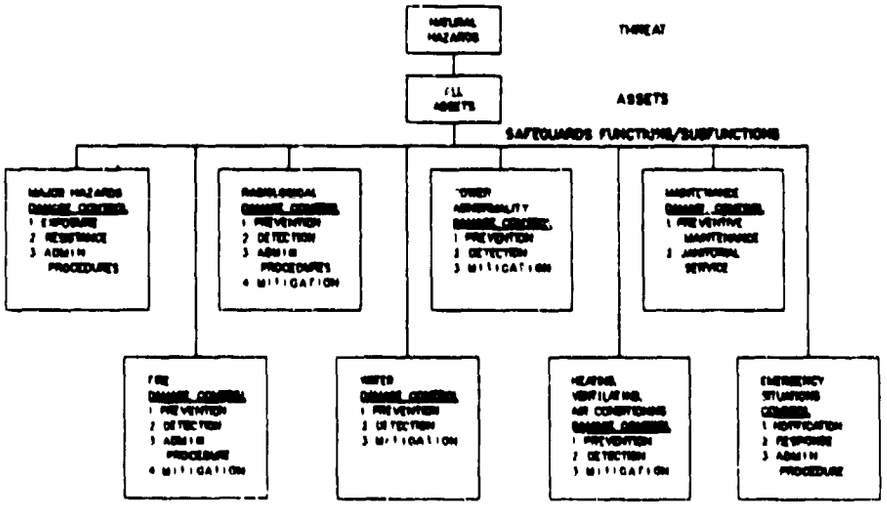

Fig 1 Hierarchical structure for natural hazards

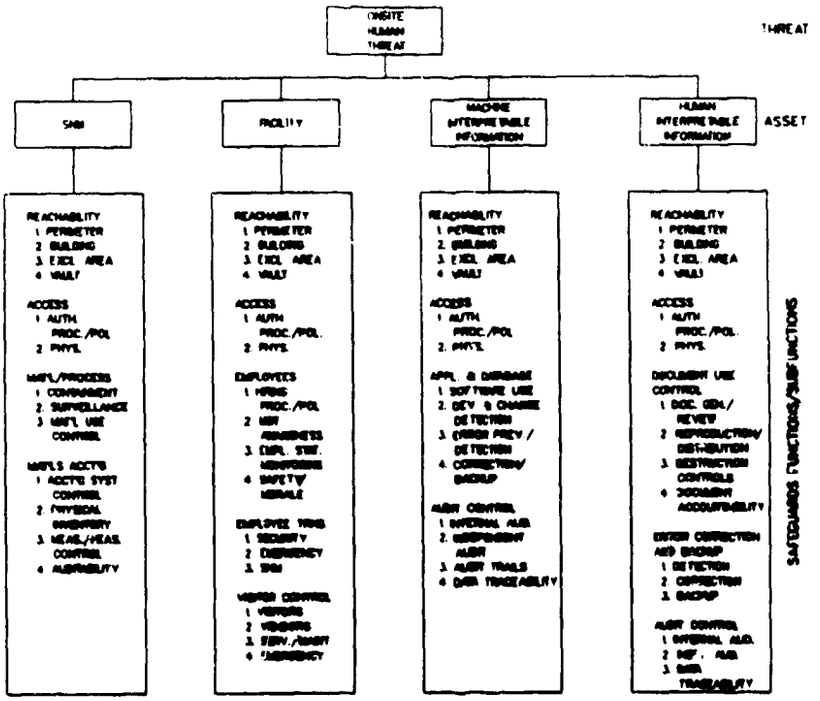

Fig. 2. Hierarchical structure for onsite human threat.

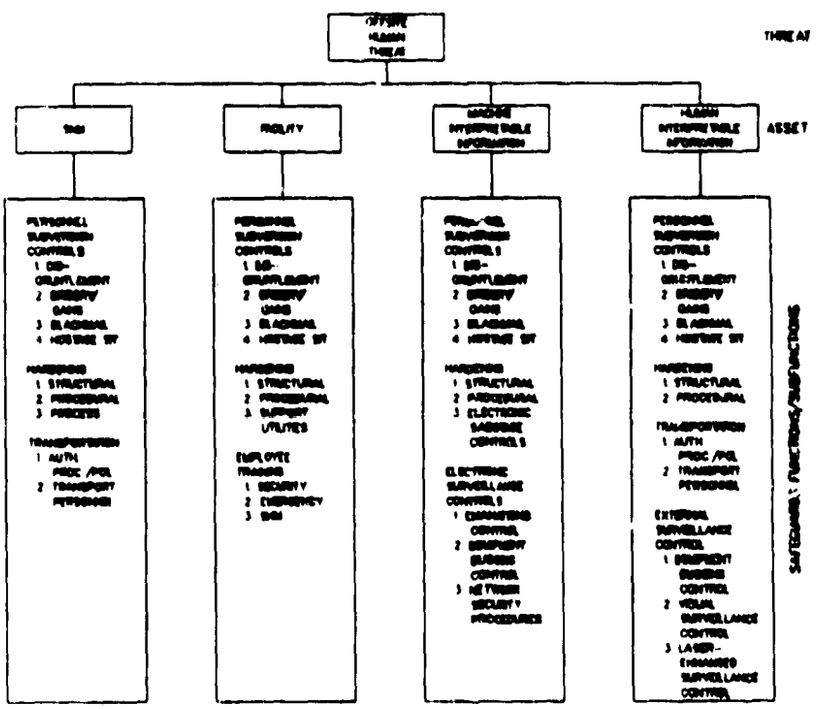

Fig. 3. Hierarchical structure for offsite human threat.

T-A PAIRS	OUTCOMES: THEFT	DIVERSION	UNAUTH CONTROL	RADIOLOGICAL SABOTAGE/ RADIOACTIVE RELEASE	DENIAL OF USE/LOSS OF PRODUC CAPABILITY	DAMAGE/ INJURY	UNAUTH MODIFI DISCLOSURE
NAT HAZ, ALL	0	0	1	1	1	1	1
ONSITE H, SNM	1	1	1	1	1	1	1
ONSITE H, FAC	1	0	1	1	1	1	1
ONSITE H, M-I INFO	1	0	1	0	1	0	1
ONSITE H, H-I INFO	1	0	1	0	1	0	1
OFFSITE H, SNM	0	0	1	1	1	1	1
OFFSITE H, FAC	0	0	1	1	1	1	1
OFFSITE H, M-I INFO	1	0	1	0	1	0	1
OFFSITE H, H-I INFO	1	0	1	0	1	0	1

Fig. 4. Outcome possibility matrix.

Once we have established the threat, asset, and outcome sets and the outcome possibility matrix, we then address what constitutes the ideal safeguards system for preventing the threats from attacking the assets and achieving the postulated outcomes. For this we define a set of safeguards functions for each of the distinguishable threat-asset pairs (nine T-A pairs, in this application) in such a way that the relative importance of each function within the set of functions for each T-A pair is about the same. Then, for each of the individual safeguards functions, we define a set of subfunctions that provide performance criteria for the adequacy and completeness of that safeguards function; each of the subfunctions is devised so that the relative importance of each subfunction within a specific function is about the same. Again referring to Figs. 1-3, the figures show the safeguards functions and subfunctions for each distinguishable threat-asset pair.

The questionnaires and other data required for the software engine to operate upon derive from the existing safeguards orders; from inspection, evaluation, and certification criteria; and from discussions with recognized experts in the field.

CONCLUSIONS

Using the LAVA approach for risk assessment of nuclear materials safeguards has benefits that do not accrue from the use of other methods. First, the automated report generators produce results that are immediately usable, both to managers who must make major, far-reaching decisions and to the security personnel in the field whose job it is to maintain an acceptable level of safeguards. Second, because LAVA produces both qualitative and quantitative results, users feel more comfortable with the results because they understand both the results and the information that produced those results. Third, because LAVA does not require the user to generate probabilities (often unfounded) for its operation but instead relies on a natural-language, user-friendly interface to acquire its data, users are more willing to act upon its results. And finally, because of the team environment in which an assessment is performed and the discussions that arise among team members, using a LAVA application has proved to be an experience that both raises the security consciousness of the users and enhances the overall working environment at the facility.

REFERENCES

1. S. T. Smith, et al., "An Automated Procedure for Performing Computer Security Risk Analysis," Proceedings Sixth Annual Symposium on Safeguards and Nuclear Material Management (European Safeguards Research and Development Association, Joint Research Centre, Ispra, Italy, 1984), ESARDA 17, pp. 527-530.

2. S. T. Smith, et al., "Risk Analysis in Computer Systems—An Automated Procedure," Information Age, Vol. 7, No. 1 (January 1985).

3. S. T. Smith, et al., "Assessment of Computer Security Effectiveness for Safe Plant Operation," Proceedings of the 1984 Annual Meeting of the American Nuclear Society, New Orleans, LA, June 3-8, 1984.

4. S. T. Smith, et al., "LAVA: A Conceptual Framework for Automated Risk Analysis," Proceedings of the 1986 Annual Meeting of the Society for Risk Analysis, Boston, MA, November 9-12, 1986.

5. S. T. Smith, et al., LAVA Methodology: Risk Assessment (A Status Report), Los Alamos National Laboratory, Safeguards Systems Group Report N-4/88-281 (May 1988).

6. S. T. Smith, et al., "LAVA for Computer Security: An Application of the Los Alamos Vulnerability and Risk Assessment Methodology, Release Version 1.01," Los Alamos National Laboratory report LA-UR-86-2942 (August 1987)

7. S. T. Smith, et al., "Application of Risk Assessment Methodology to Transborder Data Flow," Handbook for Transborder Data Flow, IDF Report, Williamsburg, VA (November 1985)