NUREG/CR-1781
SAND80-2352
RS

ASSESSMENT OF METHODS FOR EVALUATING ADEQUACY OF PHYSICAL PROTECTION SYSTEMS*

Leon D. Chapman

November 1980

Sandia National Laboratories
Albuquerque, New Mexico 87185
operated by
Sandia Corporation
for the
U.S. Department of Energy

Prepared for
Division of Safeguards, Fuel Cycle and Environmental Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1060

*Presented at the American Nuclear Society Workshop, Power Plant Security, Oakbrook, Illinois, October 5-8, 1980.

ABSTRACT

Generally, the scope of a safeguards evaluation model can efficiently address one of two issues: (1) global safeguards effectiveness or (2) vulnerability analysis for individual scenarios. A brief description of the variety of models developed in these areas will be discussed. Current generation models will be described along with an assessment of their utility and a brief look at future techniques for evaluation ill be noted.

CONTENTS

EXECUTIVE SUMMARY

A brief description of several physical protection modeling techniques is described in this paper. In general, the models are categorized according to scenario based or global effectiveness methods. The rational for development of these models is also presented. Within the paper, descriptions of the early scenario models, the improved scenario models, and current generation models are given. Current generation models such as the Safeguards Automated Facility Evaluation (SAFE) technique and the Safeguards Network Analysis Procedure (SNAP) and a combined global/scenario based modeling approach is presented.

A summary of the current status and an assessment of these models is noted along with a forecast of future techniques for the evaluation of physical protection systems. A number of references is provided to permit the interested reader to obtain more detailed information on these modeling techniques.

EARLY SCENARIO BASED MODELS

Two of the first safeguards evaluation models which were developed were the Forcible Entry Safeguards Effectiveness Model (FESEM)[1] and the Insider Safeguards Effectiveness Model (ISEM)[2]. FESEM and ISEM employ Monte-Carlo techniques to simulate a group of adversaries attacking a nuclear facility. The principle difference between these two models lies in the hypothesized threat that they are structured to address. FESEM was structured to consider primarily adversaries who do not have authorized access to the facility (outsiders) while ISEM focuses on adversaries who do have authorized access (insiders).

The focus of each of the models is defined in terms of the hypothesized threat (outsiders vs. insiders), and their internal structures reflect that difference in emphasis. For example, the neutralization (battle) submodel within FESEM can accommodate any number of adversaries. In contrast, although ISEM can consider any number of adversaries who might covertly tamper with the detection system, its neutralization submodel can accommodate only one adversary who can become engaged in combat with the security force. These Monte-Carlo simulation programs consider a single target and a single adversary path and include simple engagement models. These models also required the use of large computers.

Experience gained through the application of FESEM and ISEM provided the impetus for further safeguards methodology development. There were essentially two schools of thought regarding the most fruitful direction for further developmental work. On the one hand it was clear that the single scenario orientation of FESEM and ISEM was not amenable to an evaluation of safeguards systems considered in their entirety. That is, an evaluation of the effectiveness of a safeguards system deal with those scenarios - it is likely to imply little of the safeguards system as a whold. Consequently, a need for a global approach to the problem of evaluating safeguards system effectiveness was identified. At the other extreme, both FESEM and ISEM were criticized for not including a sufficient amount of detail in individual scenarios. This criticism was directed primarily at their inability to represent complex tactics that might be used by the adversaries as well as the security force.

To satisfy both of these concerns, developmental activities proceeded along two lines. ONe area of work centered on the development of detailed scenario models. This work resulted in a second generation of scenario models that can explicitly represent quite complex tactics. The other area of work focused on developing a global approach to safeguards effectiveness evaluation. The result of the global effort is an interlinked collection of analytical techniques which can be used to evaluate the effectiveness of the entire safeguards system. These analytical techniques allow for a significant simplification and facilitate

a global treatment of the problem. The next sections describe in more detail the products of these two developmental activities.

IMPROVED SCENARIO MODELS

The primary thrust in the development of the second generation scenario models was in the direction of enhancing the capability to represent complex tactics. This enhanced capability was pursuded through the development of two separate scenario models. One of these models, the Fixed-Site Neutralization Model (FSNM)[3], was developed with the intent of representing tactics internally in the model's logic with a minimal amount of user input of a tactical nature. The other scenario based model, the Safeguards Network Analysis Procedure (SNAP)[4], is the antithesis of FSNM with respect to the representation of tactics. SNAP requires explicit user input to represent the tactical process. Both models employ Monte-Carlo techniques to simulate randomness in the scenario. Outputs from the models include estimates for a variety of system performance measures.

Fixed-Site Neutralization Model (FSNM)

FSNM consists of a representation of the facility and personnel along with their activities and decision processes. The facility is represented in the model as a rectangular area which may, and probably should, extend beyond the boundaries of the actual facility. Architectural features of the facility, such as buildings, fences, walls, and outside areas (yards) are represented, together with interior features such as roofs, floors, stairs, doors, rooms, and walls. Such details as the visibility through a barrier, the difficulty of penetrating the barrier, and whether a door is closed or open, locked or unlocked, are explicitly modeled. The locations of sensors and their types, coverages, and operational states also appear in the facility description. The goals of the adversary are represented by specifying locations in the facility which are required to be occupied by some number of adversaries, possessing certain equipment, for a certain length of time.

Individual persons in the model, called "players", are represented in considerable detail. The representation has three aspects: physical, potential, and psychological. Adjustment of any or all of these aspects permits the simulation of differences between individuals or forces due to training, ability, or equipment. The physical aspect of a player's representation includes his location, posture, weapons and equipment, and physical status. The weapons and equipment a player carries may include pistols, rifles, grenades, light antitank weapons, ladders, keys, and other equipment. The characteristics of each type of weapon, including range, ammunition supply, and effectiveness against various targets, are represented.

Players in the model have three main activities in which they may decide to engage during a simulation time period. These activities are to move, fire, or observe. Other activities may also occur, including surrendering to or capturing an opponent. Every player has an associated collection of perceptions about observable entities (people, vehicles, and sensors) at the facility. These perceptions form, in effect, the "memory" of a player and may change as the result of direct observation by the player or by his reception of information from other players over communication systems.

Safeguards Network Analysis Procedure (SNAP)

SNAP is a simulation language developed specifically for modeling safeguards systems. With the SNAP approach, the analyst constructs a model of the safeguards system by interconnecting a set of SNAP symbols to represent the system elements and their interactions. The resulting SNAP networks are then transferred to a computer compatible form by data cards representing the symbols and their interconnections.

Using the SNAP procedure for safeguards modeling, one combines knowledge of the system, scenarios, modeling objectives, and the SNAP symbology to develop a network model of the system under consideration. This network model is a graphic representation of the nuclear facility, guard operating policies and adversary attack scenario. Typically, the elements of this network model will form a one-to-one correspondence with the components of the actual physical system and scenario being studied. Due to this relationship, a SNAP network provides an excellent communications vehicle. SNAP symbols have been designed to represent the individual elements of a nuclear safeguards system, thus the translation from a system element to the SNAP symbol should be direct.

A SNAP network model is composed of the facility subnetwork, the guard subnetwork, and the adversary subnetwork which interact to produce the overall behavior of the safeguards system. Items which flow through network models are referred to as transactions. The transactions which flow through a SNAP network are guard forces and adversary forces. The force is the most fundamental level of detail in SNAP and represents one or more individuals acting as a single unit.

The facility subnetwork is the most basic of the three networks. It is a static network in the sense that transactions do not flow through it during the simulation. Its purpose is to define the various elements of the facility and their relationships. These elements may include fences, yards, nuclear material, storage vaults, doorways, rooms, sensors, etc. The guard

subnetwork defines guard operating policies and includes a representation of the guards' decision logic as well as their physical movement through the facility. Guard forces are the transactions which flow through the guard subnetwork. The adversary subnetwork is treated in a similar manner.

The flexibility afforded by SNAP makes it the preferred approach to modeling scenarios. In effect, all of the modeling capabilities of FESEM and ISEM are included in SNAP. Moreover, if a sufficient amount of detail is incorporated into the facility, adversary, and guard submodels the level of resolution can be equal to that of FSNM. It is worth noting that the inherent flexibility of SNAP is a result of the modeling philosophy used in its development. That is, the SNAP analysis program can be viewed as a simulation "language" specially tailored to model safeguards scenarios.

With the advent of SNAP, the majority of the criticism directed at the limitations pertaining to the representation of detail of the early scenario models (FESEM and ISEM) was answered. SNAP can be used to represent quite complex tactical situations and, as a consequence, lends credibility to the evaluation of individual scenarios. In the context of "vulnerability analyses", SNAP is a valuable tool in that it can provide insights into the strengths (or weaknesses) of the safeguards system in defending against a predefined adversary scenario. However, as previously observed, the analysis of a single scenario is likely to offer little in the way of global insights with respect to the safe guards system. Moreover, even without considering analyst time, a detailed analysis of a sufficient number of scenarios to gain these global insights is unlikely to be computationally tractable. In addition, it is not obvious just what is implied by "a sufficient number of scenarios". To address these inherent limitations which are inexorably linked to any scenario based technique, a global approach to the evaluation of safeguards effectiveness was developed.

Logic Models

During this same period, logic models were developed to support the safeguards efforts. These models were primarily developed around fault tree logic. One model, the Generic Sabotage Fault Tree (GSFT)[5], was designed to identify the sabotage events which, in proper combination, can lead to the release of radioactive material from the nuclear power plant. Through the logic of the fault tree, this determination defines where in the facility a saboteur must go in order to initiate radioactive release. These areas are normally referred to as Type I and Type II vital areas within the facility. A Type I vital area is an area in which the adversary is required to visit one location in order to be successful in accomplishing the sabotage goal. Type II vital

areas are those areas in which the adversary is required to visit more than one location in order to accomplish sabotage. This technique is currently being applied to all operating nuclear power plant facilities as part of the Nuclear Regulatory Commissions' safeguards review process.

Another type of fault tree/event tree model called the Adversary Sequence Diagram (ASD)[6] was developed to address generic ways the adversary could accomplish sabotage. This technique decomposed the threat into force, stealth, and deceit and considers the most stressful situation for each component in the safeguards system. The ASD provides a logical approach to identifying vulnerabilities in the safeguards systems.

CURRENT GENERATION MODELS

The principle limitations of the scenario based models with respect to their applicability to a global safeguards effectiveness evaluation were observed to be of a philosophical as well as a technical nature. First, on the technical front, the scenario based models involve relatively complex Monte-Carlo simulation techniques. In addition to the significant amount of computer time necessary to replicate a sufficient number of times to obtain statistical stability, the time required of the safeguards analyst in preparation of the input for a single scenario can be excessive. Perhaps more importantly, the modeling philosophy of the scenario based models does not include the "generation" of adversary scenarios.

The Safeguards Automated Facility Evaluation (SAFE)[7] methodology evolved as a result of efforts to overcome the limitations described above. The technical limitations were addressed by developing a set of analytical techniques which are computer-time efficient and by structuring a highly user-oriented approach that is analyst-time efficient. On the philosophical level, techniques for generating "optimal" adversary scenarios were developed.

SAFE consists of a collection of functional modules for facility representation, component selection, adversary path analysis, and effectiveness evaluation. SAFE combines these modules into a continuous stream of operations. The technique has been implemented on an interactive computer time sharing system and makes use of computer graphics for the processing and presentation of information. Using this technique, a global evaluation of a safeguards system can be provided by systematically varying the parameters that characterize the physical protection components of a facility to reflect the perceived adversary attributes and strategy, environmental conditions, and site operational conditions.

The SAFE procedure requires as input, a blueprint of the facility, showing the facility layout characteristics, the targets, and vital areas. To obtain this input, the analyst must perform a facility characterization activity[6]. Relevant sources of information for this activity include the security plans, facility drawings, safety analysis reports, environmental reports, and site visits. Based upon this information, the analyst must synthesize the necessary facility layout characteristics, targets and vital areas, operational conditions, site-relevant environmental conditions, physical protection system and guard characteristics for which analyses are to be performed.

The first step in the application of SAFE is to construct a computer representation of the facility. This representation provides an explicit record of the analyst's assumptions concerning the facility. For example, the analyst would indicate all principle barriers and obstacles to adversary movement, all points of potential ingress and egress, floor levels and interconnections, and targets and vital areas for specific operational conditions. This information is used to organize and digitize the pertinent facility information into a computer usable form. The final output of the facility representation is a graph in which nodes represent potential access points or targets, and arcs represent possible movement between nodes.

The next phase in the SAFE analysis requires the analyst to set component performance for individual safeguards elements. The specific performance for both hardware and personnel "components" should be based upon relevant sets of environmental and adversary conditions. The analyst uses the component performance to determine weights for all nodes and arcs in terms of detection probabilities and time delays for adversary penetrations. Appropriate selection of these weights provides bounds for a range of adversary attributes. The resultant graph-theoretic representation serves as input to the adversary path analysis module within SAFE.

The generation of adversary scenarios is achieved by selecting optimal paths through the facility for the adversary. Both theft and sabotage path selection were previously accomplished by several alternative techniques[8,9,10,11]. Currently, SAFE uses one of three measures for a versary pathfinding: 1) minimum adversary task time, 2) minimum adversary detection probability, and 3) minimum timely-detection of the adversary. Within SAFE, these measures can be either deterministic[12] or stochastic[13]. In effect, the timely-detection method generates paths which minimize the probability that the security force can confront (or interrupt) the adversary. The output of the adversary path analysis is a collection of ordered sets of node identifiers that represent physical paths in the facility which are the most "critical" in terms of the measure being used. This information is a portion of the input to the effectiveness evaluation module in SAFE.

Effectiveness evaluation can be decomposed into two major parts: interruption and neutralization for a given path. The path is "evaluated" by first determining the probability that the adversary will be interrupted and then determining the probability that the adversary will be neutralized or defeated by the security force. These two probabilities can be multiplied together to yield the total probability that the physical protection system will be successful in defending against the adversary along the path under consideration.

The Estimate of Adversary Sequence Interruption (EASI)[14] model is an analytical technique which is used in the effectiveness evaluation module to compute the probability that the adversary will be interrupted. EASI focuses on the adversary path and requires information related to the probability of detecting the adversary, the time required for determining the proper response, the probability of communication with the security forces, the delay along the adversary path and the response time of the security force. The output of EASI is an estimate of the probability of adversary interruption along the specified path, i.e., the probability that the security force arrives at a point along the adversary's path prior to the time that the adversary passes through that point.

The Brief Adversary Threat Loss Estimator (BATLE)[15] model is an analytical technique that is used to estimate the probability that the adversary is neutralized by the security force. In addition to the distance between combatants, the information required by BATLE is the type of weapons, the recency of training, the amount of cover, and the number and timing of arrivals of reinforcements for the adversary as well as the security officers. The output of BATLE includes the probability that the adversary is neutralized by the security force. This "neutralization probability" is then multiplied by the "interruption probability" to yield the total probability of success of the physical protection system for the path in question.

Capabilities for effectiveness evaluation can be utilized in either a single or multipath mode. During a single path evaluation using EASI, the probability of interruption is calculated and the user may request two- or three-dimensional plots which show the probability of adversary interruption or probability of system win as a function of one or two of the input variables[16]. Based on the probability of interruption, these graphs illustrate sensitivities related to upgrading the facility. The multipath option displays in tabular form the probability of interruption, the traversal time of each path, and the frequency at which nodes appear in the set of critical paths. The multipath evaluation identifies paths that are particularly vulnerable and thus are

candidates for study by more elaborate evaluation modules such as the scenario based models previously described.

A Combined SAFE/SNAP Approach

Generally, the scope of a safeguards evaluation model can effectively address one of two issues:

1) global safeguards effectiveness, or
2) vulnerability analysis for individual scenarios

SAFE addresses 1) in that it considers the entire facility; i.e., the composite system of hardware and human components, in one "global" analysis. SNAP addresses 2) by providing a safeguards modeling symbology sufficiently flexible to represent quite complex scenarios from the standpoint of hardware interfaces with other elements of the physical protection system while also accounting for a rich variety of human decision making.

A combined SAFE/SNAP approach to the problem of safeguards evaluation logically proceeds along the following lines:

1) Initially, apply SAFE to identify global safeguards vulnerabilities,
2) Represent these vulnerabilities in scenarios that can be analyzed using SNAP.

Conceivably, insights of a global nature (especially as they relate to guard tactics and deployment strategies) could be gained from the SNAP vulnerability analysis. These insights might be formally "fedback" to SAFE, thus closing the global/scenario evaluation loop.

SURE Methodology

Another model called the Safeguards Upgrade Rule Evaluation (SURE)[17] methodology is based upon probability and utility theory concepts. The SURE method utilizes a hierarchical structure derived from a decomposition of the NRC rules (10 CFR 73.45) for fuel cycle facilities. This functional decomposition continues down to the safeguards component level. At the component level, questionnaires must be answered to assess the effect of various factors on component performances, i.e., operation, maintenance, and environmental effects on hardware and proficiency level and completeness of procedures. Ultimately, this information is aggregated through each level of the structure to arrive at an overall measure of compliance with the regulatory requirements of the NRC rules. This method allows the opinions of experts to form the basis for the input of the model. SURE also provides a very clear traceability of system performance from the component

performance level for equipment, personnel and procedures to the requirements of the rule.

CURRENT STATUS OF METHODS

For an outsider adversary with the intent of creating sabotage at a nuclear power plant, methods (SAFE and SNAP) exist to provide the anlayst with sufficient capabilities to address the important safeguards problems. Limitations exist on input data in the detection area and human performance area relative to security officers. The human responses dealing with neutralization will always be an area with insufficient data and an area for which live experiments of battles cannot be conducted to adequately validate neutralization models. Due to the complexity of physical protection problems, information gained by exercising the evaluation models should be utilized in a supplementary way for aiding the safeguards analyst in his decision making process.

For the insider reactor sabotage problem, only limited modeling techniques exist for addressing the acts of sabotage. Methods to address the detection of plant operational states which could lead to radioactive release are yet to be developed. These techniques will be addressed during FY 81 through current NRC research programs. Questions dealing with compartmentalization, access authorization, work rules, and operational impacts are only now being addressed from a research point of view.

FUTURE ASSESSMENT METHODS

The near term methods to be developed for assessment of reactor safeguards systems will encompass the decomposition of the NRC rules to the component level using a highly logical fault tree structure. This method should become available in FY 82. In addition, the Multiple Integrated Laser Engagement System (MILES)[18] will be utilized to test both the training of security officers and the security system at the nuclear power plant.

CONCLUSIONS

There currently exist adequate models for addressing the outsider reactor sabotage problem. This assessment is primarily based upon a comparison of available input data versus the level of modeling detail. Insufficient data will always exist in this area and therefore extensive detail in a given model will be of little utility. The purpose of these models must be kept in mind when one utilizes a safeguards model. If the output of the modeling analysis provides useful information for the safeguards analyst, then the models possess a high degree of utility. On the other hand, methods for addressing the insider reactor problem in a comprehensive sense are currently under development and should become available in the 1981-82 time frame.

REFERENCES

1. L. D. Chapman, et al., Users Guide for Evaluating Alternative Fixed-Site Physical Protection Systems Using "FESEM", SAND77-1367 (Albuquerque: Sandia National Laboratories, November 1977).

2. D. D. Boozer, D. Engi, Insider Safeguards Effectiveness Model (ISEM) Users Guide, SAND77-0043 (Albuquerque: Sandia National Laboratories, November 1977).

3. D. Engi, et al., Fixed-Site Neutralization Model, Volume I, Executive Summary, SAND79-0064 (Albuquerque: Sandia National Laboratories, January 1979).

4. F. H. Grant, et al., A Network Modeling and Analysis Technique for the Evaluation of Nuclear Safeguards Effectiveness, NUREG/CR-0616 (Albuquerque: Sandia National Laboratories, December 1978).

5. G. B. Varnado, Reactor Safeguards System Assessment and Design, Volume I, SAND77-0644 (Albuquerque: Sandia National Laboratories, June 1978).

6. A. E. Winblad, et al., Preliminary Engineered Safeguards System Design for a Mixed-Oxide Fuel Fabrication Facility, Volume III, SAND77-1155 (Albuquerque: Sandia National Laboratories, January 1979).

7. L. D. Chapman, et al., Safeguards Automated Facility Evaluation (SAFE) Methodology, SAND780378 (Albuquerque: Sandia National Laboratories, August 1978).

8. B. L. Hulme, Graph Theoretic Models of Theft Problems. I. The Basic Theft Model, SAND75-0595 (Albuquerque: Sandia National Laboratories, November 1975).

9. B. L. Hulme, Pathfinding in Graph-Theoretic Sabotage Models. I. Simultaneous Attack by Several Teams, SAND76-0314 (Albuquerque: Sandia National Laboratories, July 1976).

10. B. L. Hulme, D. B. Holdridge, SPTH3: A Subroutine for Finding Shortest Sabotage Paths, SAND77-1060 (Albuquerque: Sandia National Laboratories, July 1976).

11. B. L. Hulme, D. B. Holdridge, KSPTH: A Subroutine for the K Shortest Paths in a Sabotage Graph, SAND77-1165 (Albuquerque: Sandia National Laboratories, August 1977).

12. B. L. Hulme, MINDPT: A Code for Minimizing Detection Probability Up To a Given Time Away From a Sabotage Target, SAND77-2039 (Albuquerque: Sandia National Laboratories, December 1977.

13. D. Engi, J. S. Shanken, PATHfinding Simulation (PATHS) User's Guide, SAND78-2177 (Albuquerque: Sandia National Laboratories, to be published).

14. H. A. Bennett, User's Guide for Evaluating Physical Security Capabilities of Nuclear Facilities by the EASI Method, SAND77-0082 (Albuquerque: Sandia National Laboratories, June 1977).

15. D. Engi, C. P. Harlan, Brief Adversary Threat Loss Estimator BATLE) User's Guide, SAND80-0952 (Albuquerque: Sandia National Laboratories, October 1980).

16. D. W. Sasser, User's Guide for EASI Graphics, SAND78-0112 (Albuquerque: Sandia National Laboratories, March 1978).

17. H. A. Bennett, M. T. Olascoaga, Design Guidance and Evaluation Methodology for Fixed-Site Physical Protection Systems, Volume I and II, SAND79-2378 (Albuquerque: Sandia National Laboratories, March 1980).

18. R. L. Wilde, Small Force Engagement Experiment (SFEE), SAND79-2473 (Albuquerque: Sandia National Laboratories, February 1979).

DISTRIBUTION:

U.S. Nuclear Regulatory Commission (320 copies for RS)
Division of Document Control
Distribution Services Branch
7920 Norfolk Ave.
Bethesda, MD 20014

U.S. Nuclear Regulatory Commission
MS 881SS
Washington, DC 20555
Attn: M. Fadden

U.S. Nuclear Regulatory Commission (2)
MS 1130SS
Washington, DC 20555
Attn: R. Robinson

Los Alamos Scientific Laboratory
Attn: G. R. Keepin, R. A. Gore, E. P. Schlonka, D. G. Rose
Los Alamos, NM 87544

Allied-General Nuclear Services
Attn: P. E. Ebel
P.O. Box 847
Barnwell, SC 29812

Lawrence Livermore Laboratory
University of California
P.O. Box 808
Attn: A. J. Poggio
Livermore, CA 94550

Pritsker and Associates, Inc.
P.O. Box 2413
Attn: F. H. Grant
West Lafayette, In 47906

Pritsker and Associates, Inc.
P.O. Box 8345
Attn: J. Polito
Albuqurque, NM 87198

Union Carbide Corporation
P.O. Box P, MS-189, Bldg. K-1001
Union Carbide Corporation - Nuclear Division
Attn: D. Swindle
Oak Ridge, TN 37830

Naval Surface Weapons Center
Code G-42
Attn: E. Jacques
Silver Spring, MD 20910

DISTRIBUTTION (Cont.)

400	C. Winter
1000	G. A. Fowler
1230	W. L. Stevens, Attn: R. E. Smith, 1233
1700	W. C. Myre
1710	V. E. Blake, Attn: M. R. Madsen, 1714
1716	R. L. Wilde, Attn: B. D. Link, 1716
1720	C. H. Mauney, Attn: J. W. Kane, 1721, J. D. Williams, 1729
1727	V. K. Smith
1730	J. D. Kennedy, Attn: W. N. Caudle, 1734
1750	J. E. Stiegler, Attn: M. J. Eaton, 1759
1754	I. G. Waddoups, Attn: J. L. Todd, 1754
1758	C. E. Olson, Attn: D. D. Boozer, G. A. Kinemond, 1758
1760	J. Jacobs, Attn: M. N. Cravens, J. M. deMontmollin, 1760A
1761	T. A. Sellers, Attn: A. E. Winblad, J. L. Darby, 1761
1762	H. E. Hansen
1765	D. S. Miyoshi
4400	A. W. Snyder
4410	D. J. McCloskey
4413	N. R. Ortiz
4414	D. E. Bennett
4414	S. L. Daniel
4414	M. S. Hill
4414	G. B. Varnado
4416	L. D. Chapman (10)
4416	K. G. Adams
4416	J. A. Allensworth
4416	L. M Grady
4416	C. P. Harlan
4416	R. D. Jones
4416	M. T. Olascoaga
4416	C. J. Pavlakos
4416	J. M. Richardson
4416	S. L. K. Rountree
4416	D. W. Sasser
5000	J. K. Galt
5600	D. B. Shuster, Attn: A. A. Lieber, M. M. Newsom, 5620, R. C. Maydew 5630
5640	G. J. Simmons, Attn: R. J. Thompson, 5641, L. F. Shampine, 5642
5642	B. L. Hulme
8266	E. A. Aas
3141	T. L. Werner (5)
3151	W. L. Garner (3)
	For: DOE/TIC (Unlimited Release)
3154-3	R. P. Campbell (25)
	For: NRC Distribution to NTIS