Lawrence Livermore Laboratory

EVALUATION OF SAFEGUARDS PROCEDURES. A SUMMARY OF A METHODOLOGY

J. D. SALISBURY and J. W. SAVAGE

March 8, 1979

MASTER

TABLE OF CONTENTS

Acknowledgment	iv
Abstract	1
Introduction	2
Safeguards Procedures	4
Working-Level Protection Requirements	8
Generic Adversary actions	10
Generic Abnormal Situation Indications	15
Generic Responses	15
Generic Targets	16
Evaluation Process	19
Evaluation Process Steps	19
Program Status	22
Glossary of Selected Safeguard Terms	25
Appendix A	27
Appendix B	33

ACKNOWLEDGMENT

Credit for the original concept belongs to Leo R. Spogen. Many of his ideas have been retained in this report.

ABSTRACT

This report describes a methodology for the evaluation of safeguards procedures. As presently conceptualized, the methodology will consist of the following steps:

1. Expansion of the general protection requirements that are contained in the NRC regulations into more detailed but still generic requirements for use at the working level.
2. Development of techniques and formats for using the working-level requirements in an evaluation.
3. Development of a technique for converting specific facility protection procedures into a format that will allow comparison with the working-level requirements.
4. Development of an evaluation technique for comparing the facility protection procedures to determine if they meet the protection requirements.

1. INTRODUCTION

The objective of this report is to summarize a program for the NRC to develop and demonstrate an evaluation methodology for the procedures of a safeguard system. Most of the basic ideas for this methodology have been conceptualized and this report represents an overview of these ideas.

The purpose of a safeguard system is to protect against adversary actions involving threats, thefts, and sabotage relating to special nuclear materials and high-level radioactive wastes. Adversary actions* defined in this manner can be considered as general protection requirements. In order to evaluate safeguards procedures, however, it is necessary to expand these general requirements into practical working-level requirements as shown diagrammatically in Figure 1. These working-level requirements should describe adversary actions in sufficient detail such that an evaluation of the capability of safeguards procedures to protect against them can be confidently made. Furthermore, the expansion of these requirements into working-level detail should be done in such a manner that the actions and sequences represent a comprehensive set of protection requirements.

A safeguard system consists of people, mechanisms, barriers, and procedures. Because this methodology is for evaluating safeguards procedures, a separate section has been included for describing the context in which we view them. The procedures describe how the other components, i.e., people, mechanisms, and barriers, fit together and operate in order to meet safeguards protection requirements. Evaluation of safeguards procedures by the methodology summarized herein would be accomplished by means of suitably derived working-level protection requirements. That is, the procedures would

*See Glossary of Selected Safeguards Terms at the end of this report.

Figure 1. In this evaluation methodology, to determine if general protection requirements are met, the requirements would first be expanded to working-level detail and then compared with facility procedures and other pertinent data in a suitable evaluation process.

be evaluated on the basis of how well they protect against adversary actions and sequences as described by these working-level protection requirements.

The following sections of this summary will describe briefly the nature and functions of safeguards procedures, the development of working-level protection requirements, the evaluation process, and the status of development of the methodology described herein. A technique for developing adversary actions is discussed in Appendix A and some of the evaluation process techniques are illustrated in Appendix B.

2. SAFEGUARDS PROCEDURES

As mentioned previously, safeguards procedures describe how the people, mechanisms, and barriers fit together and operate to form a safeguard system. As shown in Figure 2, procedures can be classified as how to:

- A. Monitor to detect adversary actions
- B. Respond to protect against detected adversary actions, and
- C. Provide general support for these functions.

Descriptions of how to monitor and respond to detected adversary actions are the primary functions of safeguards procedures. All other procedures that support these functions, however, should be important considerations in the evaluation process. For example, the ability of a guard to detect abnormal situations (that might be induced by adversary action) and respond appropriately and effectively is in large measure dependent on his physical and mental capabilities, training, and experience. Procedures for hiring and training guard personnel should be considered, therefore, in the evaluation of safeguards procedures that involve the monitoring and response functions.

Figure 2. Two primary functions of safeguards procedures are detection and response to adversary actions. Other procedures enhance the safeguards function in a secondary or supportive way.

In order to illustrate the context in which we view safeguards procedures, we will discuss a procedure for monitoring. An example of a procedural-monitor function is the roving guard patrol for checking on the perimeter-protection integrity. In this function the patrol surveys the perimeter on a routine basis for signs of abnormal conditions. To increase the effectiveness of the patrol against adversary action based on an expected time interval between patrols, the procedure might call for a random time interval between patrols. If the perimeter barrier were backed up by adequate instrumentation to detect intrusion, the time interval of guard patrols could be correspondingly increased.

This leads to a conclusion that people and procedures can be replaced by barriers and mechanisms. And of course, the reverse is also true. That is, all functions of a safeguard system could be accomplished by people and procedures. These are the two extremes and, of course, there is a continuum of safeguards systems within these extremes. This might be a useful way to view procedures when considering what is important to their evaluation. Figure 3 illustrates this idea. It is probably obvious that people and procedures can provide all safeguards monitoring and response functions. It might be a little difficult to consider people and procedures totally replaced by barriers and mechanisms. However, the point is to emphasize the total scope of procedures as they are used in the safeguards context. That is, that they can be used for all safeguards functions and could be viewed in that context.

Figure 3 Hypothetically a safeguard system could be composed entirely of barriers and mechanisms or, people and procedures. Practically, the actual safeguard system is composed of all of these elements and the trend is toward more mechanization.

3. WORKING-LEVEL PROTECTION REQUIREMENTS

As stated previously, to determine that general requirements to protect against theft, threat, and sabotage have been met, it is necessary to reduce these requirements to the working level. By our definition, the working level is where the adversary actions and sequences are sufficiently detailed that procedures to protect against them can be confidently evaluated. Part of the task for developing these requirements will be to define the detail of the working level and this should be done in concert with persons who represent a broad experience in the present NRC evaluation processes.

Protection requirements used in this methodology are defined by means of the following:

- A. Generic adversary actions (GAA)
- B. Generic abnormal situation indications (GASI)
- C. Generic responses. (GR)
- D. Generic targets (GT)

In brief, the generic adversary actions define what the safeguard system protective elements should protect against where the protective elements are barriers and monitor/response procedures, as shown in Figure 4. That an appropriate monitor/response procedure exists can be determined by means of the generic abnormal situation indication (GASI)/generic response (GR) combinations, as indicated in Figure 5.

Thus, the protection requirements are defined first by generic adversary actions (GAA) that the adversary might use and the generic targets of these actions. Secondly, the requirements are defined by the generic abnormal situation indications (GASI) that should be produced by the GAA and the generic responses that should occur from these GASI. That is, for each GASI

Fig. 4. Working-level protection requirements can be met by using appropriate barriers and monitor/response procedures to protect against each of the generic adversary action/generic target combinations (GAA/GT)

Fig. 5. The appropriateness of a response to a monitor alarm can be verified by means of generic abnormal situations indications (GASi) and the generic response (GR) combinations.

there is a suitable GR. These requirements, in a suitable format together with a specific facility's protection means, also in similar format, form the basis for evaluating the protection means.

A. Generic Adversary Actions. In this methodology, the GAA would be derived by fault trees, as shown in Appendix A. It is convenient to define the actions as either basic or preparatory. Generic adversary action sequences (GAAS), are formed by making logically consistent combinations of these two types of actions. The basic actions describe actions in the main adversary sequence and the means to accomplish each basic action is described by a sequence of preparatory actions. Such relationship is demonstrated by example in Figure 6. The egress actions are shown for the case of sabotage initiation by time delay or by offsite means. Similar lists can be shown for the main sequences of adversary actions for theft or threat objectives. The basic actions for sabotage would include actions such as those defined in Table I.

Each of the actions in a main sequence would be performed by some method as shown in Figure 7. For example, in order to access the protected area, Action 1 of Figure 6, the adversary might choose to use falsified personal identification to deceive the access control system. Thus, the adversary method would be deception and the means to achieve deception would, in the general case, require a set of preparatory actions. Adversary methods, such as those defined in Table II, would be used for the various adversary actions in a sequence.

As stated, each of the adversary methods requires some preparatory actions as means to accomplish it and these preparatory actions can be developed by means of fault trees.

Figure 6 Example of basic actions and supporting preparatory actions that an adversary would use to accomplish a sabotage objective.

TABLE I. Example basic actions for sabotage

1. Access protected area. An adversary action to enter the facility by means of a personnel portal, vehicle portal, perimeter barrier penetration, etc.
2. Access vital area. An adversary action to enter the vital area by means of a portal or by penetrating a barrier.
3. Act against primary target. In the case of sabotage, this is an adversary action against one or more vital parts of a facility to cause radioactive release.
4. Prevent damage control. An adversary action with intent to block or otherwise prevent facility actions to minimize the effects of the sabotage action.
5. Egress vital area. An adversary action to leave the vital area by means of a portal or by penetrating a barrier.
6. Egress protected area. An adversary action to leave the facility by means of a personnel portal, a vehicle portal, perimeter barrier penetration, etc.

Figure 7 Examples of adversary methods for accomplishing basic actions. A sequence of preparatory actions for one of the methods is used by the adversary to develop the means to accomplish the basic action.

TABLE II. Examples of Adversary-Action Methods

1. Stealth. An adversary action method to avoid detection of his/her presence or act.
2. Deception. An adversary method to accomplish an unauthorized action in what appears to be a normal or authorized way.
3. Covert force. An adversary method which uses force in a concealed manner. For example, the penetration of a barrier surreptitiously.
4. Overt force. An adversary method to accomplish an unauthorized action by means of unconcealed use of force such as an armed assault against a guard force at an access portal.

B. Generic Abnormal Situation Indications. Preparatory actions might be conducted onsite, offsite, or both ways. The basic actions and onsite preparatory actions are detectable in principle. Whether or not they are detected depends on the sensitivity of the safeguards procedures and mechanisms to detect the abnormal situation indications which these adversary actions produce. Of course, response procedures against an adversary action can only be initiated if the action is detected. Therefore, the first step in protecting against adversary actions and sequences is the use of appropriate monitoring mechanisms and/or procedures to provide indications of these actions. The second step is to appropriately respond to the indications. The nature of the response depends upon the nature of the indication. For example, an indication of possible adversary action may be highly reliable, or, oppositely, the indication may be of low reliability and probably a false alarm. Obviously, the response procedures to these indications should be considerably different. The first indication should call for an immediate guard-force reaction to interrupt and neutralize the adversary. Whereas, the second indication should call for a response procedure to determine if the indication was adversary induced.

As mentioned before, the existence of appropriate monitor/response combinations can be determined by a comparison with pertinent GASI/GR combinations. A technique for making this comparison is described in Appendix B. Examples of generic responses are discussed in the next section.

C. Generic Responses. Predetermined response procedures should exist for all abnormal situation indications (ASI). The predetermined response to an "event" or ASI is the essence of contingency planning. That is, in planning for contingencies, it is essential to minimize the chances that a

significant "event" might not be planned for which, if it occurred, would require an ad hoc decision/action process to determine what response to make.

A response to an indication of possible adversary action would entail taking steps to deter, delay, or prevent further actions and eventually neutralize the adversary. Generically, these response procedures can be described as follows:

1. Get more information.
2. Increase chances of detection (of following generic actions).
3. Cause delay (in the execution time of following generic actions).
4. Prevent (the occurrence of following generic actions), or
5. Neutralize the adversary (directly or following any combination of the above).

For example, unless the abnormal situation indication leaves no doubt as to the intentions of an adversary, the response procedure to a first indication would be to get more information. At the same time, it might be logical to increase the chances of detection by turning on additional lights if at night, by sending a search party, and/or by increasing the facility alert status. If the objective (sequence or partial sequence) of the adversary group is known or suspected, responses might be to cause delay or prevent subsequent actions and eventually interrupt and neutralize the group.

The response procedures will include a responsibility matrix which will identify responsible individuals/organizations (operational elements) and their decisions/actions.

D. Generic Targets. The adversary objective is achieved by a sequence of adversary actions. The actions are against targets which we define as primary and secondary in the following manner:

1. A primary target if acted against successfully by the adversary could result in release of radioactivity or theft of material (SNM or HLW).
2. A secondary target is one which must be overcome in order for the adversary to act against the primary target. These secondary targets would be the protective elements of a safeguard system, such as, people, procedures, devices, and barriers that control access to the PH and VA.

Examples of adversary targets are shown in Table III.

TABLE III. Examples of Adversary Targets

Primary Targets of Sabotage of Power Reactor

1. Reactor Coolant System
2. Engineered Safety Features
3. Containment

Secondary Targets (For various methods)

1. Access Authorization System
 - a. Guards
 - b. Automated Personnel I.D. (Badge Reader)
2. Contraband Detection System
 - a. Metal Detector
 - b. Explosives Detector
 - c. Package Search
3. Perimeter Protection System
 - a. Roving Patrol
 - b. Surveillance with moving target indicator
 - c. Proximity sensors

4. EVALUATION PROCESS

As was shown in Figure 1, the evaluation process is the means by which facility procedures and data are examined to determine if the working-level protection requirements have been met. The techniques to be used in this evaluation have been conceptualized, but some of their details remain to be developed as outlined in LLL's 189 proposal, "Safeguard System Decision Logic Evaluation Methodology, Rev. 2," 6/7/78. Therefore, the following discussion will emphasize what the process is intended to do rather than how it is to be done. Appendix B describes some of the "how" techniques that might be used.

To evaluate a procedure, it is necessary to determine:

- Why it is needed. That is, what protection requirement it is supposed to meet.
- What it does to meet the protection requirement. That is, if it addresses each part of the protection requirement.
- If it provides adequate means to satisfy the protection requirement.

A. Evaluation Process Steps. In brief, the evaluation process will consist of the following:

1. As part of the methodology development, matrices of generic adversary preparatory actions (for each adversary method) and generic targets will be provided for each basic action, such as those shown in Figure 6 for sabotage. Implausible action/target combinations in each matrix will be deleted.

2. The evaluator would prepare these action/target matrices for use in evaluating a specific facility by deleting additional action/target combinations that did not apply because of facility design characteristics. The remaining generic action/generic target combinations of each matrix would

represent what the facility should protect against. So the next part of this process will be to determine what protective means the facility uses against each adversary action and if the means are appropriate and adequate.

3. From the preceding matrices, evaluation of protection will be done by determining what barriers and/or monitor/response procedures are used as protection means. The evaluator will determine if the barrier protection requirements are met by examining the characteristics of the barriers and the procedures for monitoring their integrity.

4. The suitability and adequacy of monitor/response combinations will be determined by a technique such as a decision table. This will compare the important characteristics (quantity, quality, and type of information) of the abnormal situation indications (ASI), which derive from the procedures for monitoring, with the procedures for responding. That is, each facility-produced ASI should have a suitable response based on the characteristics of the ASI.

For purposes of illustration, let us assume that the evaluator is considering the protection procedures against adversary action to gain access to the protected area (PA) by using deception means (falsified picture badge) against the PA access control system. In order to gain access to the protected area by the deception method, the means to deceive the system must be developed by the adversary. This requires a preparatory sequence of actions which might be conducted totally offsite, totally onsite with the assistance of an insider, or a combination of both.

Depending on the adversary capability and knowledge, the falsified identification badge might be made entirely by the adversary with available resources. On the other hand, because of special processes and materials used

in construction of these badges by an outside firm, the adversary might find it necessary to steal the badge material from this firm. Thus, offsite theft might be a necessary part of the preparatory sequence. Similarly, if the badges are constructed entirely onsite in a way that cannot be duplicated by the adversary, acquisition of this material would require insider assistance.

Evaluation Considerations: The foregoing basic and preparatory action examples illustrate the way that protection requirements could be developed for use by an evaluator. To evaluate procedures for protecting against this basic action, the methodology will provide evaluation considerations such as the following:

1. What are the facility procedures for perimeter access control at the personnel portal? Are the badges made so that chances of falsification are satisfactorily low?
 2. If the badges are made entirely onsite, are suitable means taken to prevent theft of blank badges or material?
 3. If badges are made partially or totally offsite, are suitable control procedures required of the manufacturer to protect against theft?
 4. If a card reader and computer-controlled identification system are used, are there security measures against compromise of this system?
- Etc.

Facility Conditions. An important consideration in the evaluation process is the effect of facility conditions other than normal operating conditions. When assessing the protection against a particular generic action or sequence, the evaluation process will consider whether or not the protection will be degraded significantly by unusual facility conditions. Examples of unusual facility conditions include the following:

1. Refueling
2. Maintenance
3. Start up or shutdown
4. Guard force strike
5. Internal emergency
6. External emergency
7. Local natural disaster

Although refueling and maintenance conditions might be handled adequately by existing procedures, other conditions, like the ones shown, might not have been prepared for. For example, the safeguard system protection might be degraded by a guard force strike. Also, local law enforcement assistance (LLEA) might be significantly degraded or not available during a local natural disaster or offsite emergency. An offsite emergency might be precipitated by an adversary group as a diversionary means to support its subsequent acts against the facility. It is important, therefore, to understand and account for the level of outside assistance that would be available in these kinds of situations.

In brief, the evaluation process will be designed to assist the evaluator by presenting in a convenient fashion the important things to be considered as illustrated by the foregoing examples.

5. PROGRAM STATUS

The objective of this program is to develop and demonstrate an evaluation concept for the procedures of a safeguard system. Most of the basic ideas for this evaluation methodology have been conceptualized and this report represents an overview of these ideas.

The next step in this program is to develop the subtasks of the methodology as outlined in LLL's draft proposal to NRC of June 6, 1978. As part of the conceptualization, some of the subtasks have been started. For example, in the development of generic adversary actions and sequences, fault trees appear to be a useful technique. Fault trees have been used for preliminary development of some preparatory sequences, as described in Appendix A. Other ways of developing and representing adversary actions and sequences, such as matrices, have attractive features also. No optimal approach has emerged yet and the initial development might best be achieved by a combination of various techniques. Other potentially useful techniques to represent and analyze data were examined as a result of the conceptualization. These techniques include, generic action/generic target matrices, target/target matrices, and decision-table representation for abnormal-situation-indication/generic-response analysis. Some of these are described in Appendix B.

One of the attractive features of fault-tree use for adversary actions and sequences is the existing, well developed computer capability at LLL and elsewhere to analyze fault trees. A useful characteristic of the computer code is that generic adversary action sequences that do not meet protection requirements could be generated and listed in order of their importance in correcting protection inadequacies. However, this feature requires that the evaluation of protection against an action/target combination be specified as the probability of adversary success. Since present evaluations are not made in terms of quantitative probability numbers, this feature is a future capability.

From the work done so far in the development of working-level protection requirements, such as, adversary actions, it seems likely that the level of detail in their description will be subject to individual preference. For example, some generic adversary actions involving deception have been developed to what appears to be a useful working level. Whether this level is too high or too low is best resolved by user interaction. To this end, LLL has submitted a proposal to work with Inspection and Enforcement personnel through the Operational Support Branch of the Division of Safeguards, Fuel Cycle, and Environmental Research.

GLOSSARY OF SELECTED SAFEGUARDS TERMS

Abnormal Situation Indication: Indication of possible adversary action.

Adversary: An individual or an organized group intending to cause adverse societal consequences or to threaten public health and safety or national security through acts involving nuclear material.

Adversary Action: One of a set of actions which an adversary must complete to produce an end event.

Adversary Action Sequence: An ordered set of adversary actions which commences with the decision to produce an end event and terminates with the occurrence of an end event.

Barrier: A physical enclosure used to protect against unauthorized access, such as a fence or locked room.

Basic Action: One of the adversary actions that is basic to the production of the end event, such as, "gain access to vital area."

Card Reader: An automated means to read the identification code in a personnel-identification badge. The card reader is associated with a central computer.

Computer Controlled Identification System: An automated means of identifying authorized personnel. At LLL, the personal identification picture badge contains a concealed code number which is read by inserting the badge in a card reader. The code number is then compared by the computer with stored code numbers which identify authorized personnel.

Contingency Plan: A document that provides guidance to licensee personnel and identifies procedures to accomplish specific, defined objectives in the event of threats, theft, or sabotage relating to special nuclear materials, high

level radioactive wastes and nuclear facilities.

Contraband: Unauthorized material or equipment that is necessary to produce the end event.

Insider: An employee of a facility or a person with authorized access who is conducting or supporting adversary actions.

Mechanism: A safeguards device for protection against adversary actions, such as, a closed-circuit TV monitor, intrusion detector, etc.

Monitor: A mechanism or human for detecting abnormal situations that might be caused by adversary actions.

Portal: An access area or entrance for personnel or vehicles with means of personnel identification and contraband detection.

Preparatory Actions: Adversary actions to prepare the means to accomplish a basic action.

APPENDIX A

DEVELOPMENT OF GENERIC ADVERSARY ACTIONS

The reason for developing adversary actions was outlined in the section on "Working-Level Requirements." In that section, it was pointed out that the general requirements to protect against threat, theft, and sabotage are specified by more detailed working-level requirements which are derived from the generic adversary actions. By specifying these requirements in greater detail, evaluation of the protection procedures against them can be made more confidently.

We have chosen the fault-tree technique for developing generic adversary actions. Part of the development effort proposed by LLL will be to develop a complete set of generic adversary action fault trees. This technique is a means for systematic and logical development of adversary actions. The fault tree also serves as a useful way to display the actions and their relationship to each other and to the adversary primary objective of threat, theft, or sabotage. From Figure A-1, it can be seen that the primary objective, in this case "Sabotage Pri. Targets," can be achieved by; (1) acting against one or more primary targets, and (2) preventing the facility's efforts to control the damage caused by the sabotage action. (Explanation of the fault-tree symbols is given in Table A-1.)

Action against a primary target requires access to it and the means to commit the action. Each of these actions is basic and requires preparatory actions, as was shown in Figure 6. Since, in this case, the adversary primary objective is sabotage, the means to effect the sabotage action would be described by a sequence of preparatory actions. (In fault-tree style, an

FIG. A-1 BASIC-ACTION FAULT TREE FOR SABOTAGE

<u>Symbol Description</u> Rectangle	<u>Event Description</u> Gate event
Diamond	Event not further developed
Oval	Basic event (Basic action)
OR Gate	Q exists if one or more inputs exist
AND Gate	Q exists only if all inputs exist

Table A-1. Fault-tree symbol description

undeveloped sequence of actions is represented by a diamond symbol.) When developed, the actions will specify the steps that an adversary might use to prepare and emplace the sabotage means. For example, if the sabotage means were developed offsite, the necessary actions to introduce these means into the vital area will be shown on the fault tree. This, of course, would include introducing the means into the protected area (PA).

Continuation of fault tree development will proceed as shown in Figure A-2. Here the rectangle (top event) was taken from the corresponding diamond in the lower left corner of Figure A-1 and partial development was started to illustrate how this will be done. In order to accomplish the event specified by the rectangle in Figure A-2, it is necessary to select an adversary method, viz., deception, stealth, covert force, or overt force. For example, if the adversary were to choose to act against the PA access target by deception in order to enter the facility, he/she would develop the means to do this by a sequence of actions. The left hand diamond of Figure A-2 represents this undeveloped part of the fault tree which when developed will show generically the preparatory actions that an adversary might use. Each of the diamonds in this figure and in Figure A-1 will be developed as indicated.

From the completed fault tree the basic and preparatory actions will then be used to specify working-level protection requirements in suitable format. As indicated in the section on the evaluation process this could include a set of considerations that an evaluator would use in the evaluation. The evaluation will be completed for a basic adversary action when the evaluator is confident that protection against that action is adequate for each adversary method and for all facility conditions.

Fault trees for sabotage and theft have been partially constructed. (To illustrate the fault-tree technique, a part of the sabotage fault tree was used for Figure A-1.)

Figure A-2 The adversary means to act against the PA access target is developed by a sequence of preparatory actions which these diamonds represent. Each diamond represents a sequence for an adversary method.

APPENDIX B

ILLUSTRATION OF THE EVALUATION PROCESS

I. Evaluation Techniques

As stated in Section 4, Evaluation Process, the means by which facility procedures and data are examined to determine if the working-level protection requirements have been met can be facilitated by a variety of techniques. The following discusses a combination of two of these techniques which have emerged as showing the most promise for use in this methodology. They are a generic adversary action/target (GAA/GT) matrix technique together with a generic abnormal situation indication/response (GASI/GR) decision table technique.

The GAA/GT matrix will be reduced from an all-encompassing reference listing in a manner which is illustrated in Step 1 of Figure B-1; first to fit a facility type and then further reduced to correspond to a specific facility of that type. The reduction for facility type will be accomplished as part of the methodology development. The further reduction for a specific facility will be accomplished by the evaluator.

The GASI/GR decision table is a technique to assist the evaluator in determining the appropriateness of facility response procedures to facility-generated indications of abnormal situations. The evaluator uses this table during the evaluation of facility protection against a particular generic adversary action, as illustrated in Step 2 of Figure B-1.

Step 1
Definition of Protection
Requirements

Step 2
Evaluation of Protection
Provided by Facility Safeguard System

Figure 8-1 Steps in the Evaluation Procedure

Thus, the action/target matrix specifies facility protection requirements and the decision table assists the evaluator in his evaluation of the protection against the adversary actions. The evaluation proceeds as shown in Step 2 of Figure B-1. That is, each action/target combination is examined with respect to passive protection, such as barriers, or active protection, such as monitor/response procedures, or a combination of both of these active and passive methods.

A. Protection Requirements for a Facility Type. To develop protection requirements for a facility type, reference lists of adversary actions and targets, such as those shown in Figure B-2, for example, will be developed. These will be further expanded, as in Figure B-3, until sufficient detail exists to comprehensively cover the facility type being evaluated, which in this case is a power reactor.

The comprehensive GAA/GT list will then be formed into a set of matrices. Figure B-4 shows the format of an action/target (A/T) matrix for the basic action, gain access to the protected area (PA), where the rows are actions and the columns are targets in the access control system. The actions shown are preparatory for each method needed to accomplish a basic action. That is, there are preparatory actions for each of the adversary methods, such as overt force, covert force, deception, and stealth, that an adversary would use to expedite his accomplishment of the basic action. In order to illustrate the nature of preparatory actions the matrix of Figure B-4 includes tampering. This action is typical of one the adversary might use to alter the access control system so as to aid him in gaining access to the PA.

In Figure B-4, the "X" marks are used to illustrate the adversary-action/target combinations that do not apply to the specific

<u>Generic Actions</u>	<u>Generic Targets</u>
<u>Actions Against Primary Targets</u>	(X) SNM
Access	(X) Waste
(X) Acquisition	Reactor Coolant System
Sabotage (Destroy, Disable)	Engineered Safety Features
	Containment
<u>Actions Against Secondary Targets</u>	Access Control System
Access	PA (E)
(X) Material Removal	VA
Tampering	(X) SNM Process Equipment
Egress	Power System
Other	Normal
	Emergency
<u>Action Type (apply to actions listed)</u>	Control System
Authorized	Physical Security System
Unauthorized	Contraband Detection System (E)
<u>Action Methods (apply to types listed)</u>	Communications System
Force	LLEA System
Overt	Procedures
Covert	Routine
Deception	Nonroutine
Stealth	Containment Control
	Nuclear Plant
<u>Adversary Type (apply to methods listed)</u>	(X) Processing Plant
Insider	Intrusion Detection System (E)
Outsider	PA
	VA
<u>Contraband Used (apply to adversary type)</u>	System Integrity System
Yes	Maintenance
No	Testing
	Inspection (Patrol)

NOTE: (1) This list is not intended to be complete.
 (2) (X) = Does not apply to Power Reactor.
 (3) (E) = Expanded in Figure B-3.

Figure B-2 Example of Action and Target Lists Modified for Use with Power Reactors.

(Protection requirements which will be put in the A/T Matrix are synthesized from these lists.)

P.A. Access Control System

Guard Inspection
Barriers
Roving Patrol
Proximity Sensors
(X) Automated Badge Reader
(X) Computer ID System Hardware
(X) Computer ID System Software
Coded Locks
Conventional Locks
Key Control System

Contraband Detection System

Metal Detection
Radiation Detection
Explosives Detection
Search Procedures

Intrusion Detection System

Entry Sensors
Occupancy Sensors

(X) = Does not apply to this specific power reactor.

Figure B-3 Expansion of Selected Generic Target Details Shown in Figure B-2

PARAMETERS FOR
PROTECTION REQUIREMENTS

Basic Action - Access to PA

		TARGETS										
		Access Control System										
		Guard Inspection	Roving Patrol	Proximity Sensors	Automated Badge Reader	Computerized ID System	Hardware	Software	Barriers	Coded Locks	Conventional Locks	Key Control Systems
PREPARATORY ACTIONS	PREPARATORY ACTIONS											
	Authorized Access											
	Unauthorized Access, Using											
	Methods	Overt Force										
		Covert Force										
		Deception										
		Stealth										
	Tampering, Using											
	Methods	Overt Force										
		Covert Force										
		Deception										
		Stealth										

(This table shows Preparatory Actions
in support of the Basic Action)

☒ = DOES NOT APPLY TO FACILITY

☐ = REQUIRED TO BE PROTECTED

Fig. B-4 Partial example of generic adversary action/generic target matrix,
representing protection requirements for a specific facility.

facility that is being evaluated. In other words, the blank squares designate those adversary-action/target combinations that the facility is required to protect against by suitable procedures. Similar matrices will be made for each basic action as shown in Figure B-5. The evaluator will consider each of these protective requirements for each basic-action matrix, and each of these matrices will be evaluated by considering the impact of factors such as facility condition and adversary type.

B. GASI/GR Decision Table. In conducting the evaluation, each applicable adversary-action/target combination will be analyzed to determine if suitable protection against it is provided by the facility. This protection will be in the form of barriers and/or monitor/response procedures. Determination of the suitability of monitor/response procedures will be accomplished by use of a decision table, such as that illustrated in Figure B-6a. The evaluator will use a methodology-developed decision table of generic abnormal situation indications (GASI) and generic responses (GR) to compare with facility-generated abnormal situation indications (ASI) and response procedures, such as that illustrated in Figure B-6b.

The methodology-generated decision table will characterize each GASI as to its features, viz., quantity, quality, and type of information that it represents. These features will be expanded under the heading "Characteristics of GASI," as implied in Figure B-6a. From these characteristics, the "Decision Logic Rules" will be derived to determine the type of "Generic Response" that should be provided. If in the evaluator's judgment the facility-response procedure corresponds to the generic response, then the decision logic will be appropriate. Conversely, the decision logic may be inappropriate or the facility-generated ASI may be insufficient or both

Basic Actions	Protection Requirements
Access PA	
Access VA	
Act against pri target	
Prevent damage control	
Egress VA	
Egress PA

Fig B-5 Representation of a set of protection requirement matrix charts.

Characteristics of GASI	Decision Logic Rules					
	A	B	C	•	•	•
1	X					
2 }		X				
3 }		X				
4 }			X			
5 }			X			
6 }			X			
•						
Generic Response Procedure						
A	X					
B		X				
C			X			
•						
•						

In order to determine the appropriateness of a response, GASI characteristics to be considered are,

- Type of information (visual, audible, monitor signal)
- Quantity (number of each)
- Quality (uncertain, good, excellent)

A given GASI will result in an appropriate response, according to the applicable decision rule.

Fig. B-6a Example of a GASI/GR Decision Logic Table

INDICATION	ASI	Decision Logic Rules				
		A	B	C	D	---
Door Open	(1)	X				
Hole in Fence	2)		X			
Window Open	3)		X			
Observe Adversary	4)			X		
Floor Switch Alarm	5)			X		
Sound of Explosion	6)			X		
⋮	n					
RESPONSE						
Get more information	1 ←	X				
Increase detection	2) ←		X			
Cause delay	3)		X			
⋮						
Neutralize adversary	m ←			X		

This facility ASI / Response decision logic table will be classified into generic form for comparison with the GASI/GR decision logic table, Fig. B-6a. Characteristics of the indications will include Type, Quantity and Quality.

Fig. B- 6b Example of a Facility Decision Logic Table

conditions may exist. The GASI/GR decision table will then support the evaluator in the process of arriving at this judgment.

C. The use of the above techniques in the actual determination of protection will be made using subjective evaluation techniques. The use of objective evaluation techniques will require further development.

11. Evaluation Process

In the following, emphasis will be on an adversary action by action and target by target basis.

In performing an evaluation, the evaluator will do the following:

1. Determine the Safeguard System (SS) protection requirements for the facility being evaluated.

2. Evaluate the protection provided by the facility safeguard system.

There are two aspects to Step 2, (A) what is planned, and (B) what is achieved.

- (A) Planned protection - determine whether all of the protection requirements are recognized and planned for.

- (B) Protection achieved - determine if the protection requirements have been met.

Each of these items will be discussed in more detail.

STEP 1 - Determination of Facility Safeguard System Protection Requirements

Protection requirements are defined as the protection which the facility safeguard system must provide against adversary actions.

To determine the protection requirements for a particular facility, the evaluator will begin with reference lists of generic adversary actions and generic targets developed from the fault trees described in Appendix A, and

which will be provided in the Methodology, Figure B-2. The reference lists will cover all types of facilities and items which do not apply to the facility being evaluated will be removed. This screening will be done in two stages.

In the first stage, an initial screening will remove from consideration the actions and targets which do not apply because of facility type. (Examples of facility type are, power reactor, fabrication plant, reprocessing plant.) An example of this is shown in Figure B-2, where actions and targets which do not apply to a power reactor are marked with an (X).

In the second stage, a second screening will remove from consideration the actions and targets which do not apply because of facility design. In Figure B-3, selected generic target categories from Figure B-2 have been expanded to show more detail, and targets which do not apply because of specific power reactor design are marked with an (X).

The second screening process can be visualized more easily if the action/target list is placed in a matrix format. For this example, the access control system was selected, and is illustrated in Figure B-4, where the action/target (AT) combinations which are to be removed are marked with an (X). Combinations which remain will define the protection requirements for the facility. For instance, consideration of authorized access action against the guards and roving patrols part of the access control system is removed from the list because there is no direct way for them to detect that the access authorization has been falsified. Protection against an illegally obtained access authorization would, instead, be analyzed in the category of, say, unauthorized access using deception, which is shown in another part of

the table. The evaluator will remove other inapplicable A/T combinations from the list in a similar way.

For the limited example of Figure B-4, the protection requirements are now defined by the unmarked squares. These action/target combinations must be evaluated for completeness and adequacy as will be described later.

It should be noted that, in order to use any of the action methods listed in Figure B-4, say deception, the adversary will make preparations which could involve additional actions against other targets in the safeguard system, and these A/T combinations must also be protected against. They are omitted from Figure B-4, for simplicity, but will be included in the A/T matrix provided in the methodology.

Factors Which Affect SS Protection

The performance of the protective means* provided to satisfy the facility protection requirements will be affected by several important parameters such as:

1. Basic action description
2. Adversary type
3. Facility operating condition (normal, refuel, guard strike, etc.)
4. Adversary objective (theft, sabotage)
5. Etc.

The first of these is shown in Figure B-4 as, Gain Access to PA. It is essential for the evaluator to consider the others also, and the working

*The protective means are barriers, monitors, SS responses, procedures, decision logic, LLEA responses.

matrix will include them as parameters which are shown in the upper left hand corner of Figure B-7.

The balance of the requirements for the facility being evaluated will be determined by repeating the steps just described. Upon completion of Step 1, the evaluator will have constructed a family of matrix charts which contain blank squares for each action/target combination against which protection is required as illustrated in Figure B-5. The charts will be indexed in a way that will identify all special conditions and other parameters which might affect the evaluation of the safeguard system procedures.

STEP 2 - Determination of Protection Provided by Facility SS

The protection means provided by the safeguard system can be classified into two categories:

(1) Passive means

Barriers

Support procedures

Etc.

(2) Active means

Monitors

ASI

Responses

(1) The first category includes those means which protect against adversary actions by virtue of their inherent capability, such as barriers and support procedures, etc. They function in a predetermined way with little or no interaction with other parts of the SS and no adaptation to specific circumstances. For classification reasons they are called passive, and their protection performance is design dependent.

(2) The second category involves active protection means in which there is interaction among various parts of the SS, such as monitor-initiated responses (GASI and GR). For classification reasons these are called active,

PARAMETERS FOR
PROTECTION REQUIREMENTS

- o Adversary Objective - Sabotage
- o Basic Action - Access To PA
- o Adversary Type - Outsider
- o Facility Condition - Normal
- o Adversary Uses Contraband

		TARGETS									
		Access Control System									
		Guard Inspection	Roving Patrol	Proximity Sensors	Automated Badge Reader	Computerized ID System	Hardware	"	"	Software	
PREPARATORY ACTIONS	PREPARATORY ACTIONS										
	Authorized Access										
	Unauthorized Access, Using										
	Methods	Overt Force			X	X	X		X		
		Covert Force			X	X	X		X		
		Deception			X	X	X		X		
		Stealth			X	X	X		X		
	Tampering, Using										
	Methods	Overt Force	X	X		X	X	X	X		
		Covert Force	X	X		X	X	X	X		
		Deception	X	X		X	X	X	X		
		Stealth	X	X		X	X	X	X		

(This table covers Preparatory Actions in support of the Basic Action)

☒ = DOES NOT APPLY TO FACILITY

☐ = REQUIRED TO BE PROTECTED

Fig. B-7 Partial example of generic adversary action - generic target matrix, representing protection requirements for a specific facility.

and their performance might be influenced by altering the interactions and responses.

These two categories can be extended into a more complex realm, wherein protection against sequences of two or more action/target combinations can be analyzed by using techniques which must be developed. Protection will be determined by considering combinations of two or more protection methods which were not acceptable on an individual basis.

An adversary encounter with passive protective means can be illustrated as follows:

The barrier may resist alone, if the adversary is unobserved, or in combination with an active system response, if the adversary is detected.

The execution of active protective means, which will be initiated following observation of an abnormal situation, can be illustrated as follows:

The above sequence of steps must occur in order for the active part of the SS to function against an adversary. Therefore, the sequence identifies the basic procedures which the evaluator must consider in order to evaluate the system.

There are two aspects to the evaluation.

Aspect A: Whether protection is provided against all required action/target combinations.

Aspect B: Whether the protection provided meets protection requirements.

ASPECT A

In this aspect the evaluator will compare the facility SS procedures with the protection requirements to determine if there is adequate agreement on an item by item basis.

SS protection will exist in the form of barriers, to deter the adversary and/or responses to an indication of an adversary action. The

latter will be executed according to a contingency plan which relates the indication (event) to an appropriate response which will neutralize the adversary. The part of the SS which relates the ASI's and SS responses, is called Decision Logic, and its evaluation is accomplished by use of a generic table relating GASI to GR.

The evaluator will determine the following:

- If there are (a) monitor procedures provided to detect the adversary actions or, (b) protective barriers provided to deter the adversary.
- If the monitor procedure generates a reliable abnormal situation indication (ASI).
- If the ASI initiates an appropriate SS response procedure.
- If the specified response procedure and/or barrier provides protection against the adversary attempt.

In the conduct of the evaluation, the steps will be to:

- (1) Tabulate in generic form the monitor procedures or barriers provided by the facility SS.
- (2) Examine protection requirement action/target matrices, and identify, for each action/target combination, (a) the procedure to detect it, or (b) the barrier to protect it.
- (3) Tabulate indications (ASI) provided by monitors, in generic form (GASI). Include type, quantity and quality information for the ASI.
- (4) Tabulate responses in generic form (GR).
- (5) Construct the Decision Logic table from (3) and (4).

The methodology will supply the evaluator with generic reference tables of barriers, monitors, abnormal situation indications, and responses which will guide him in classifying specific facility data in the generic form.

Examples of decision logic tables are shown in Figures B-6a and B-6b. Figure B-6a includes a listing of type, quantity, and quality of GASI characteristics which must be considered in order to determine the appropriateness of responses.

ASPECT B

This aspect consists of the determination of the adequacy of protection provided by the SS against each of the adversary action/target combinations listed in charts similar to Figure B-7. It will require the evaluator to consider each of the parameters and protection requirements in sufficient detail to match the type of analysis being performed, and to take into consideration the nature and completeness of data available. For example, a conceptual analysis may require only generic data, whereas a very detailed analysis would require very detailed specific facility data which would be included in expanded charts.

The evaluator will consider whether or not the protection is degraded significantly by any listed parameters, and the methodology is intended to encourage the evaluator to supplement the reference tables with additional factors which he may feel are significant.

Determination of Performance

The evaluation can be made in one of three ways:

- (1) Subjectively, by the analyst or a panel of experts, wherein performance is determined based on expert judgment.

(2) Objectively, based on calculations or tests of SS performance which consider all significant factors which influence the chances of neutralizing the adversary attempt. These factors would be the same as were selected for the subjective evaluation, but performance data must be available or be obtained by test. (Methodologies developed by others can be used for some of these factors.) This type of evaluation requires developmental work by LLL to determine the manner in which the factors would be combined to calculate the performance value.

(3) A combination of (1) and (2), which uses available data in combination with subjectively determined performance.

Acceptance criteria, in any case, would be specified by NRC. The protection against each A/T combination could be stated on a "pass-fail" basis or on a scale of 1 to 5, for example. A value less than the predetermined acceptance criteria would be cause for rejection.

Example - Using Access Control System

As previously described, the evaluation will determine if protection is provided against each action/target combination remaining in the chart of Figure B-5. Using information from applicant submittal, interviews, and inspections, the evaluator will use his expertise to make a judgment and score the SS for each action/target combination shown in the protection requirements.

In order to simplify the example the combinations which are acceptable are marked in Figure B-8 with an A, and those which are not with an O.

In the example, it is obvious that the access control system is vulnerable to any use of force by the adversary, and the system would be rejected unless acceptable protection were provided by other parts of the SS to make up for the deficiencies of the access control system.

PARAMETERS FOR PROTECTION REQUIREMENTS

- Adversary Objective - Sabotage
- Basic Action - Access to PA
- Adversary Type - Outsider
- Facility Condition - Normal
- Adversary Uses Contraband

PARAMETERS FOR PROTECTION REQUIREMENTS		TARGETS										
		Access Control System										
		Guard Inspection	Roving Patrol	Proximity Sensors	Automated Badge Reader	Computerized ID System	Hardware	Software	Barriers	Coded Locks	Conventional Locks	Key Control Systems
Adversary Objective - Sabotage												
Basic Action - Access to PA												
Adversary Type - Outsider												
Facility Condition - Normal												
Adversary Uses Contraband												

(This table covers Preparatory Actions in support of the Basic Action)

A = ACCEPTABLE PROTECTION

0 = NOT ACCEPTABLE

Fig. B-8 TABULATION OF SYSTEM PERFORMANCE

When the protection against all required action/target combinations have been determined, one of two conditions will result:

1. All protection requirements are met.
2. Some protection requirements are not met.

Condition (1) means that the analysis is complete, and the SS is acceptable.

Condition (2) requires that a decision be made to either reject the system, or extend the analysis into the more complex realm wherein system plans for multiple predetermined responses to abnormal situation indications are evaluated.

Summary

The evaluation procedure just described is arranged to be a workable method for NRC evaluators to determine if a facility safeguard system satisfies protection requirements.

The evaluator can adjust the amount of detail considered to meet his needs, the nature and amount of data available, and any special conditions which might influence system performance. The evaluation can be made subjectively using techniques presently available. With further development the methodology can be expanded to accommodate more objective and complex evaluations, which could use performance data or field test data.