NUREG-0270

GUIDELINE FOR THE DEVELOPMENT OF A METHODOLOGY FOR MEASURING LEVEL OF EFFECTIVENESS OF PHYSICAL PROTECTION FACILITIES AT FIXED-SITE FACILITIES

The MITRE Corporation
for
U. S. Nuclear Regulatory Commission

NUREG-0270

GUIDELINE FOR THE DEVELOPMENT OF A METHODOLOGY FOR MEASURING LEVEL OF EFFECTIVENESS OF PHYSICAL PROTECTION FACILITIES AT FIXED-SITE FACILITIES

Wolf Haberman, and Others

Manuscript Completed: June 1977
Date Published: January 1978

The MITRE Corporation
P.O. Box 208
Bedford, MA 01730

Division of Safeguards, Fuel Cycle and Environmental Research
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Under Contract No. AT(49-24)-0376

ABSTRACT

These technical guidelines contain recommendations for a program that would utilize data obtained by NRC inspectors to measure the effectiveness of fixed-site physical protection components/systems for various levels of adversary threats. The contribution of both equipment and procedures to the measured level of effectiveness are considered. The study was conducted in response to Task 3 of NRC contract AT(49-24)-0376, and this report is submitted in fulfillment of that requirement.

TABLE OF CONTENTS

TABLE OF CONTENTS (Concl'd)

LIST OF ILLUSTRATIONS

SECTION I

INTRODUCTION

PURPOSE OF GUIDELINES

The U. S. Nuclear Regulatory Commission (NRC) has as its mission the promulgation and enforcement of regulations having the purpose of protecting the health and safety of the public with respect to commercial operations within the nuclear fuel cycle. One aspect of this mission is to ensure the physical protection of fixed facilities producing or utilizing special nuclear materials (defined in 10 CFR 50 and 70).[1]* The rules and regulations concerning how the protection should be provided are covered in 10 CFR 73 and in a series of NRC Regulatory Guides.[2] To ensure compliance with these, the NRC reviews a Physical Security Plan (PSP) submitted by each licensee and inspects each facility. At present the effectiveness of a planned or installed physical protection system for a particular adversary threat is determined by exercising a subjective judgment based upon the experience and knowledge of the individual or group reviewing the PSP or performing the inspection.

Recently, a program has been established by NRC under the cognizance of the Office of Nuclear Regulatory Research that has as its objective the development of a simulation model for physical protection systems at fixed-site facilities.[3,4,5] This model will provide the basis for determining expected levels of effectiveness for generalized (or site-specific) protection systems as an aid in the licensing process. However, there is also a need to

---

*See Appendix II for list of references. Appendix III contains a bibliography of other documents consulted.

develop a methodology that can be used to asses the actual system effectiveness achieved at a specific facility based upon measurements made by inspectors in the field. The guidelines contained herein have been prepared, therefore, to indicate how such a method should be developed to permit inspectors to determine quantitatively the effectiveness of an operating system for standard adversary threat levels defined by NRC.

It is important to point out that the level of effectiveness of an entire system to protect the health and safety of the public, which is the primary objective of NRC, must also take into consideration the effectiveness of special nuclear material control procedures including SNM accountability, transportation security (transfer of SNM to a vehicle, in-transit protection, etc.), and related administrative and operational procedures. However, these guidelines will only address the effectiveness of the on-site physical protection system. This includes both equipment and the administrative and operational procedures employed by guards and others in the protection process.

DEFINITION OF MEASURES OF EFFECTIVENESS

Effectiveness can be defined as the extent to which a system is predicted to, or in the case under consideration, actually does achieve the objectives for which it was developed. It is a means of measuring on either an absolute or relative scale the ability of that system to perform its function with respect to a specific set of conditions. In general, system effectiveness depends upon the availability of a system at the time it is needed to perform its function, the dependability of the system to continue operating during the period of performance, and the overall capability that the system possesses to satisfy design objectives.[6]

An effectiveness measurement can be represented in several ways. For example, it can be stated as an overall figure-of-merit that provides a measure of the degree to which the system or an element of the system achieves or can be predicted to achieve success; for physical protection, this is the equivalent of the system's ability to prevent adversary mission success. Alternatively, effectiveness can be evaluated by examining the success of various sub-missions, which for protection include the expected ability of the system to detect, delay, deter and neutralize the adversary threat. In developing these guidelines for measuring system effectiveness, both types of definitions will be employed. The sub-mission effectiveness measures should be established and then combined appropriately into a single overall figure-of-merit.

DEFINITION OF A FIXED-SITE PHYSICAL PROTECTION SYSTEM

For the purposes of these guidelines, a fixed-site physical protection system includes the following:

(1) Barrier structures that can be expected to impede or delay the progress of an adversary (either external or internal) in effecting his mission objective (primarily theft of SNM or sabotage of vital areas to the extent that radioactive material will be released into the environment).

(2) Intrusion detection sensors, both those around the perimeter of protected, vital and material access areas and those in the interior of such areas.

(3) Access control devices used in the control of personnel into or out of the three types of areas.

(4) Contraband detection devices used in the process of determining that individuals entering controlled areas through normal access points do not possess weapons or explosives and that those leaving material access areas do not possess unauthorized amounts of SNM.

(5) Surveillance and alarm assessment devices (primarily closed circuit television--CCTV) used to ascertain the cause of an alarm and the level of threat presented by an adversary or to provide remote visual control over a perimeter or area.

(6) Guard forces used instead of electronic equipment to perform any or all of the functions indicated above.

(7) Ancillary equipment such as communications, displays and automated response devices.

(8) Administrative procedures concerned with and affecting site security.

(9) Operational procedures used by the guard force in detecting, assessing, communicating, and responding to a threat affecting the controlled areas of the facility.

The specific configurations that a physical protection system can take are as varied as the facilities being protected and their peculiar environments. A list of several such systems covering a range of protection capabilities is given in Appendix I. These are illustrative of what might be expected to be included among the facilities whose effectiveness is to be evaluated, although in an actual facility the likelihood is low that any of the systems would be found with exactly the capabilities and equipment as stated. However, in preparing the methodology required by these guidelines, the listed configurations can and should be used as a basis for model/algorithm design.

To reiterate, the methodology to be developed in accordance with these guidelines is not expected to cover two other safeguards aspects: material control and accounting equipment and procedures for SNM, although these may overlap to some extent with equipment and procedures used for physical protection; and transportation security of SNM from the point of transfer to a vehicle, during transit and up to the point of off-loading, except where the

fixed-site physical protection system plays a secondary role in providing security in the first and last stages of this process.

INFORMATION REQUIRED FOR EFFECTIVENESS MEASURES

To establish a measure of the level of protection afforded a specific commercial nuclear facility by a physical security system, certain data must first be ascertained. Quantitative or quantified data must be taken that represent the actual performance achieved as measured for barrier structures, intrusion detection and contraband sensors, entry (access) control equipment and procedures, communications, displays guard forces and local law enforcement authority forces. These data must then be related to an expected threat (set of adversary characteristics) to make them meaningful in terms of the level of system/component effectiveness achieved. Therefore, a range of such threats must be established and specific combinations of adversary characteristics selected against which the performance of the physical security equipment and procedures can be measured. A model (either computerized or otherwise defined) must be utilized to relate the performance measurement to the facility, and to develop, through appropriate algorithms, the level of effectiveness actually achieved. These aspects of the problem of measuring effectiveness are discussed in the balance of these guidelines.

SECTION II

MEASURES OF EFFECTIVENESS

HIERARCHY OF EFFECTIVENESS MEASURES

In developing the methodology for measuring levels of system effectiveness, it is important to keep in mind that there is a hierarchy of objectives for a fixed-site physical protection system.[7] As indicated in Figure 1, the primary objective of the total safeguards program is to protect the health and safety of the public. All methods of determining effectiveness, and measures used in that determination, must be consistent with that objective. At the next lower order, there are two goals that are directly affected by the physical protection system (as well as by the other two elements of the safeguards program). These are: (1) to prevent diversion or theft of strategic quantities of SNM, and (2) to prevent release of radio-active materials into the environment in such a way as to endanger the public. To accomplish each of these goals, the physical protection system, including both equipment and personnel, must be able to detect intruders, delay or deter their access to vital or material access areas, and finally neutralize the intrusion attempt. This must be accomplished for adversaries that act from a point external to the facility and attempt to enter by force, stealth or deceit and also for those that act from a point within the facility, regardless of their position, level of authority, or authorization, except that unauthorized removal of SNM by means not meant to be protected by a physical protection system (e.g., where material control systems are appropriate) is not included in this definition.

The effectiveness measures to be developed are to be determined for each of this last group of objectives, based on the specific data collected by inspectors in the field. These measures will be a function of the assumed adversary characteristics used in the model selected

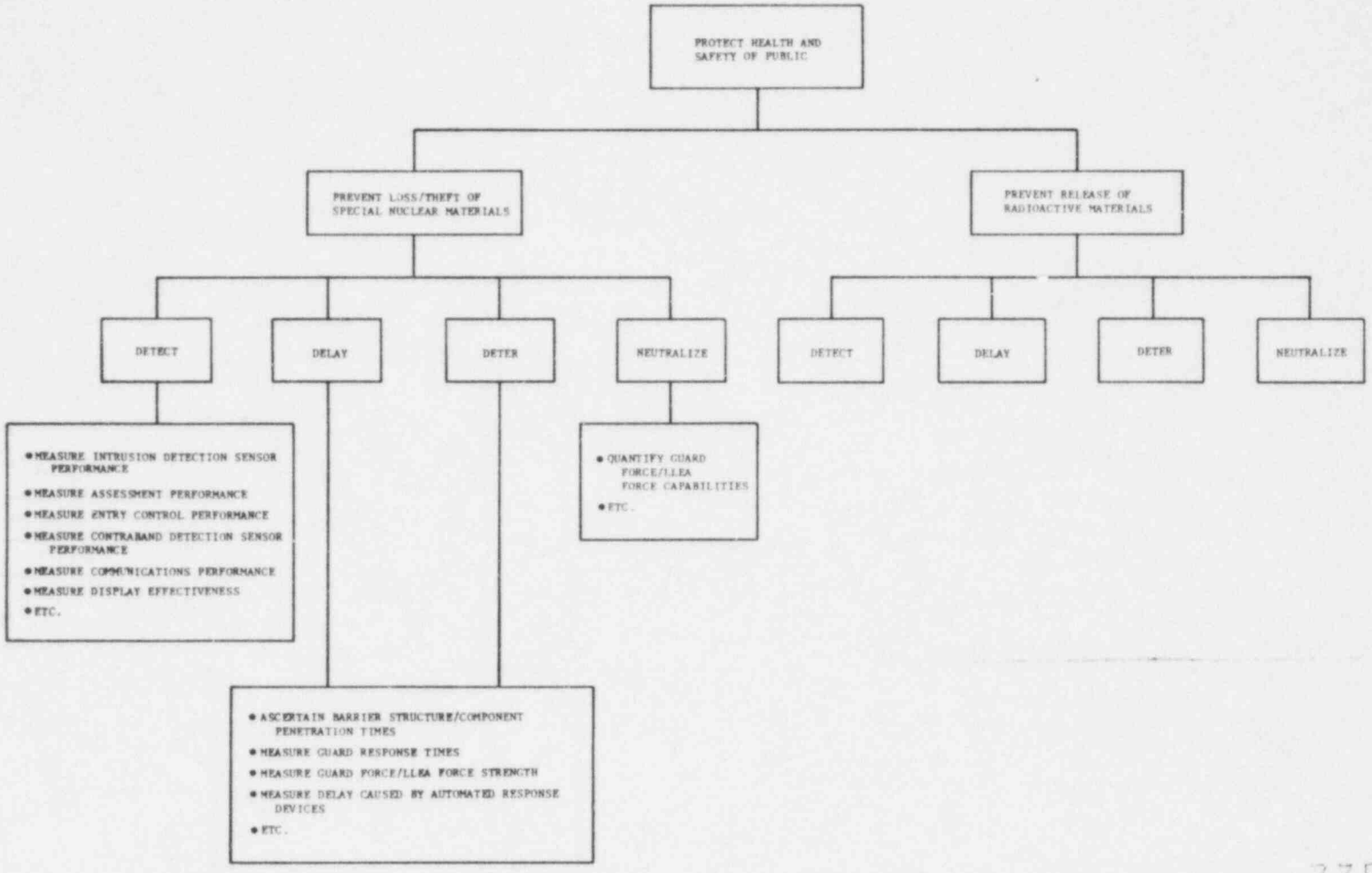

Figure 1. Hierarchy

by NRC for prediction of system effectiveness and of the formulation of both the model itself and the algorithms used to convert collected data into appropriate and acceptable simulation model inputs. As the effectiveness of each barrier structure, each item of equipment and each security procedure is determined, this information should be used in the model to compute the higher orders of effectiveness measures within the overall hierarchy. These guidelines, however, call only for the development of a methodology that will convert quantitative or quantified data collected by inspectors into a form that can be utilized by a model still in development. Further refinement of these guidelines may be necessary to ensure compatibility of the results with the final model as developed.

DISCUSSION OF HIGHER ORDER MEASURES OF EFFECTIVENESS

The single value for measuring the level of effectiveness of any safeguards system should be a figure-of-merit, which can be expressed as a probability value, giving the likelihood of preventing the complete or partial success of an adversary mission. For a physical protection system, the above overall measure of effectiveness (MOE) will be a weighted combination of four other measures: one representing the probability that an adversary will be detected by the system; a second that he (they) will be delayed by the system for the time necessary to respond; a third that he (they) will be deterred (prevented) by elements of the system (primarily barriers and guards and not by psychological factors) from successful completion of their mission; and/or a fourth that he (they) will be neutralized by a response force prior to completion of the mission. It must be recognized that the probability of neutralization is conditional in part on the probabilities of detection and delay of adversary actions. In each case, of course, the actual level of effectiveness of a system will be a function

of the size and characteristics of the adversary or group of adversaries. This will be discussed in more detail in a later section.

Components of each MOE should be comprised of measures of the availability of each critical element (barrier structures, detection equipment, communications, guard forces, response forces, etc.) as appropriate at the start of an adversary mission, the dependability of these elements during a mission to continue performing, and the level to which each element of the system is capable of performing its assigned function and to which it contributes to the higher order functions discussed above. Availability of an element, whether equipment or personnel, can be defined as a percentage of any period of time that it is expected to be in operational readiness. This is usually defined for equipment as $A_{O_E} = \frac{MTBF}{MTBF + MTTR}$

where

A_O = Operational availability

MTBF = Mean time between equipment failure

MTTR = Mean time to repair equipment after it has failed (including detection of failure, fault isolation and administrative or logistic supply time)

For personnel availability, a similar relationship can be used that combines probability factors of alertness (P_A), being at an assigned station (P_{OS}), and having the necessary inputs to act on or tools to work with (P_I). As an example, $A_{O_P} = P_A \cdot P_{OS} \cdot P_I$ would be a reasonable formulation of the above.

Dependability is closely related to availability since it is a measure of whether the equipment and personnel can be expected to continue to perform their function after the start of an adversary mission. It is a combination of the probability that the various

equipment elements will not fail and that the guard force will remain able to monitor and respond to alarms during the period of intrusion into and within the facility. Therefore, operational dependability D_O might be formulated as

$$D_O(t) = \prod_{n=1}^{m} \prod_{N=1}^{M} \left[1 - P_{f_n}(t)\right] \left[1 - P_{F_N}(t)\right]$$

where

P_{f_n} = The probability of equipment element n failing during any period of time

P_{F_N} = The probability of any guard force element N being unable to perform during that period of time.

Other more suitable formulations that weigh specific elements in accordance with their relative importance to the physical protection system during an adversary mission should be developed as part of the generalized methodology to be used in deriving an MOE.

The capability of the physical protection system to perform its function is a complex measurement dependent on the performance levels of the elements that comprise the system and the way in which they interrelate. It is this area that requires the most study in order to develop an MOE for each element as a function of the adversary threat that may be presented. After a determination is made of the contribution of each element's performance to the total system performance, these contributions can be expressed in an algorithm that defines the level of effectiveness at the next higher level in the hierarchy of objectives. The basis for these individual element MOE's will be data collected in the field by inspectors using the Equipment Evaluation Guide prepared by the MITRE Corporation for NRC[9] or a similar document dealing with administrative and operational procedures, which remains to be developed. Some of the aspects of the performance data to be considered in an MOE are described in Section III.

OTHER CONSIDERATIONS AND PROBLEMS

In developing the methodology for measuring effectiveness levels, several specific pitfalls should be avoided or consideration given to specific points:[7,8]

(1) The MOE formulation selected must be broad enough to include all significant contributions to the system or equipment effectiveness, but not so broad that meaningless data must be obtained by inspectors or estimated by others in order to complete all inputs to the algorithm being used.

(2) Pertinent objectives and portions of the MOE algorithm should not be ignored because of difficulties involved in quantifying them.

(3) The weighting given to specific elements of the MOE must have a rigorous and substantiated basis and not be arbitrarily assigned.

(4) It is important that all elements contributing to a specific MOE and the selection of the MOE itself be related to and adequately represent the objectives as shown in Figure 1.

(5) All probable adversary characteristics must be examined to determine their potential variations and their pertinence to each MOE and its component elements.

SECTION III

DATA INPUTS

The NRC inspectors will utilize all or parts of the Guide for Evaluation of Physical Protection Equipment[9] or similar documentation for physical protection procedures to determine how well specific components/elements of a licensee's physical protection system are performing. In some instances quantitative data will be taken directly; in others, subjective judgments will be made that must be quantified for use in developing a measure of effectiveness. Appropriate checklists designed to differentiate among several levels of capability should be developed to assist the inspector in this quantification process. These measurements or performance values are to serve as the input data for the algorithms to be developed as part of the overall effectiveness measurement methodology (see Figure 2).

EQUIPMENT

The following summarizes what an NRC inspector should be able to measure through tests or ascertain from visual inspections, analyses, or demonstrations.[10] It then indicates how the information developed by the inspectors is to be employed in developing the appropriate algorithms related to effectiveness. Only those parameters directly affecting security are considered.

Barrier Structures

(a) The inspector should be able to ascertain the type of structure, its material, thickness, etc., from architect/engineering drawings. He can then determine or estimate a penetration time as a function of the number of adversaries assumed in the threat and the tools they are assumed to possess by using pre-established charts such as those provided in the Catalog of Physical Protection

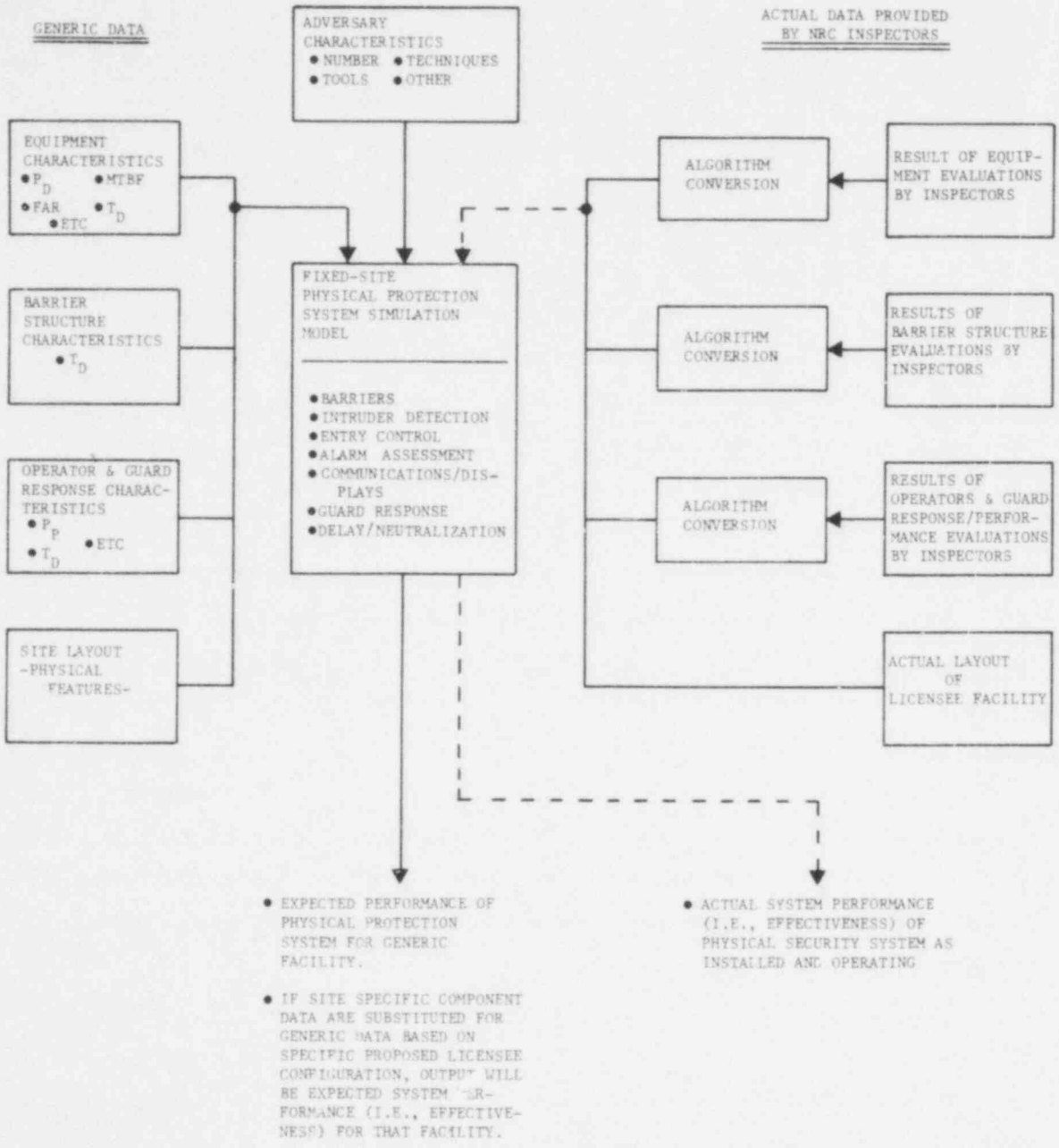

Figure 2. Generation of Expected and Actual Levels of System Performance Effectiveness.

Equipment.[11] Penetration time for perimeter fences should consider the time required to climb over, tunnel under, bridge or cut through the fabric. The specific action to be used by an adversary would be a function of the type of sensors around the perimeter and on the fence, if any. Perimeter wall penetration time should consider the time to climb over or break through the structure and also take sensor usage into account in determining the most likely adversary tactic. Gates in the perimeter should be treated as fences, walls, etc., as appropriate, except that the ability of any adversary to penetrate the lock, and the time involved, should also be included in the measure. If windows are located in the perimeter wall, consideration in computing penetration time is to be given to the protection afforded the windows (e.g., sensor alarms on windows, metal guards on windows, use of bullet resistant or unbreakable glass such as LEXAN, etc.). Similar estimates of penetration time, appropriately modified, are to be assessed for interior structures including building wall, roof, floor and window materials, vaults, doors with frames, hinges and locks, etc., using a method similar to that developed for perimeter structures.

(b) It should be possible for the inspector to assess structural integrity, tamper resistance and degradation qualitatively and then quantify them using a checklist established for that purpose. Penetration times established above should be modified as a result of this determination.

The MOE for delay and deterrence should incorporate an algorithm utilizing the modified penetration times outlined above. The precise measurements/calculations and associated checklists for quantifying any subjective judgments should be developed as part of the effort to determine the overall methodology.

Sensors

(a) The sensitivity of sensors, whether perimeter sensors, internal sensors or contraband detection sensors can be measured by inspectors, and the level then related to probability of detection (P_d) for the assumed threat. This relationship must be developed through independent tests and evaluations of the sensors and are not considered part of the effort for developing an equipment MOE. The value of P_d so determined should be utilized in the detection MOE algorithm.

(b) Availability and dependability factors for sensors should be determined based upon data ascertained through examining failure and repair records and the computed times for MTBF and MTTR. Downtime caused by power failure and factors accounting for the ability of the sensors to switch to back-up power if necessary should be included in the algorithm relating availability and dependability to the MOE for detection.

(c) Environmental factors that affect sensors within the system should be assessed through a comparison of the limitations imposed by the manufacturers or as determined through independent evaluations within the actual environment. Environments that are at or beyond the defined limits for the equipment will affect performance and must be considered in determining the appropriate MOE and its associated algorithm.

(d) The influence that sensor performance has on overall system effectiveness will be affected by factors representing: its vulnerability to spoofing, tampering and other countermeasures; its limitations, such as adversary characteristics or types of threats (materials or chemicals for contraband detectors) that will not be detected (or detected with degraded P_d); and its susceptibility to sources of nuisance alarms and false alarms because of the effect of these on sensor performance credibility. Checklists

must be developed for use by the inspector that will enable him to subjectively quantify these factors in such a way that they can be incorporated into the detection MOE algorithm.

(e) Where guards or other personnel are used to perform the detection function through continuous or routine surveillance of an area or protected perimeter or by means of periodic patrol, a checklist of factors affecting their performance must be developed for use by inspectors and the results quantified and translated into a P_d for the various adversary threats to be considered.

Access/Entry Control

(a) The time delay provided by the vulnerability of locks must be considered under barrier structures, since they primarily affect the MOE for delay and deterrance and are a function of the type of lock and bolt used for a particular door or gate. Alternatives available to an adversary in accessing an area through a door that is locked are a function of the integrity of and time delays caused by the door frame, hinges and door structural material; therefore, these must all be considered as a group in developing the appropriate algorithm.

(b) The use of coded locks or secure combination locks will contribute to delay or deterrence; however, the degree to which those codes/combinations are controlled or may become known to unauthorized personnel will affect their capability and performance. An inspector would have to examine pertinent records and make certain subjective judgments, the results of which would be used in arriving at the level of effectiveness. These factors must be taken into consideration in the development of an MOE for both delay and deterrence.

(c) Coded cards may have certain vulnerabilities to duplication and can be lost or stolen. If the card is used by itself in a system, these factors must be considered. In addition, reading

errors may occur that would permit entry of an unauthorized individual. The extent to which this may occur would most likely have to be determined from independent tests and evaluations. Note that for entry/access control devices, false rejection of an authorized individual (Type I errors), although important to a licensee (as would be processing time and system capacity), is not a factor that is usually critical to security considerations.

(d) If more sophisticated identity verification techniques are used, particularly those utilizing personal characteristics as the identifier, the Type II error rate that can be achieved (the percent of false acceptances of unauthorized individuals) must be ascertained. This error rate would generally be a function of the thresholds being used in the verification algorithm, and it would be determined by correlation with data established through independent tests and evaluations. As indicated above, Type I errors are not critical in establishing an MOE.

(e) When guards are utilized together with picture badges, the security of the badges and the level of guard performance is important. Checklists that will permit quantification of inspector's subjective judgments must be prepared to assist in measuring the effectiveness of this type of entry/access control security.

(f) In all cases, the level of effectiveness achievable must take into account such factors as availability, including ability to switch to back-up power when appropriate, environmental compatability, and tamper and spoof-proof features. The effect of these factors must be considered in the selection and derivation of the appropriate MOE.

Surveillance and Alarm Assessment

(a) A measurement can be made by inspectors of the actual volume/area being covered by CCTV cameras, and this can be compared to the volume/area under surveillance. The effectiveness of such

a system is to be developed and incorporated as part of the detection MOE.

(b) A second factor that can be ascertained by the inspector is whether the resolution at maximum range is sufficient for detection (e.g., a man should be 8 TV lines wide as a minimum for video assessment). Effectiveness should be based on a ratio of actual resolution at maximum distance to minimum acceptable resolution.

(c) Illumination levels and point-to-point variation measurements made by inspectors must be compared to acceptable standards[11] for both CCTV and visual observation surveillance, and the resultant data should be included in the MOE for detection.

(d) The "quality" of the video picture shown on the TV monitor must be ascertained through a quantized subjective judgment on the part of the inspector. Interference signals, poor synchronization and a number of other factors will affect his assessment of the picture quality. The results should be incorporated appropriately into the MOE for detection.

(e) Since a guard or operator will be performing the surveillance and alarm assessment functions, his performance must be ascertained through the use by an inspector of properly prepared checklists; the results should then be incorporated into the MOE. Factors such as ability to perceive targets, weather effects, etc., are to be considered.

(f) Other factors will also affect the MOE and modify the final determination of a level of component/system effectiveness. As was the case for other elements of the physical protection system, these factors include equipment and guard availability, environmental suitability of equipment, power switchover to back-up capability when appropriate, incorporation of tamper and spoof-resistant features, guard/operator response time from alarm to assessment, and communication of results to a response force and/or a local law enforcement authority.

Communications

(a) For analog or digital hardwire lines or video cable links, the effectiveness of any line supervision technique is critical to the overall MOE for both detection and deterrence. This effectiveness will be a function of the type of line supervision employed, its operating reliability, and the sophistication of the adversary to defeat the technique used.

(b) When installed lines have a high level of, or frequent, interference resulting in a noisy line, too little amplification or too much signal loss (thus giving a poor signal-to-noise ratio), these effects must be considered in developing an MOE based upon measurements made by inspectors.

(c) For RF links, the ratio of design transmission distance to maximum required distance, modified by potential for interference as determined in the field (from measurements of or analysis of records of incomprehensible transmissions) and other similar considerations, must be utilized in arriving at the appropriate MOE algorithm.

(d) For all links, vailability factors, environmental factors, channel capacity compared to required bandwidth, transmission delays encountered, etc., must be incorporated into the appropriate MOE to arrive at a true effectiveness level.

Displays

Devices which present alarm or assessment information to guards or a central alarm monitoring station operator are also critical to the effectiveness of a system. One important element of the MOE will be based upon comments by the guards/operators on their ability to perceive an alarm situation rapidly and to initiate the appropriate response. Actual response delays caused by the inadequacies of the display must be considered in the algorithm used in measuring display performance, along with many of the more general aspects listed above under other equipment elements.

ADMINISTRATIVE AND OPERATIONAL PROCEDURES

An important element that must be considered in the development of an MOE is the contribution that various security procedures make to the overall system effectiveness. These procedures may be operational or administrative; examples of both kinds are presented below. The capability of a security system to meet its objectives is heavily dependent on how good the procedures are and how well they are carried out. The evaluation of procedures by NRC inspectors can be highly subjective, and some means is needed to quantify these judgments so that the individual effectiveness for each procedure can be utilized in arriving at an overall MOE through use of appropriate algorithms. Therefore, all of the significant procedures used in a physical protection system must be identified and methods for evaluating them developed.(10) This evaluation methodology would, as described earlier, involve the development of checklists that enable an inspector to compare the appropriate evaluation criteria with his best judgment of the procedure used and how it is carried out. This may involve the assessment of many factors, which would then have to be combined in an appropriately weighted fashion to arrive at a quantified measurement of the effectiveness of that procedure. An example of such a list would be one that is often used in evaluating the performance of personnel in industry or in government (Personnel Effectiveness Reports used in the military services).

Prior to the work to be done in accordance with these guidelines for developing an MOE methodology, a catalog of physical protection procedures and a guide for their evaluation must be prepared.(10) Such material should then be used as a starting point to prepare the detailed checklists needed to quantify the level of capability achieved by the various operational and administrative procedures.

Administrative Procedures

Certain procedures that affect security system performance can be considered administrative in nature. A few examples of these are:

(a) Methods utilized to identify an individual and his or her authorization to be given access to vital areas or material access areas. This includes the procedures for controlling the distribution of picture badges, keys, code numbers/combinations or coded cards and for determining that an individual is eligible to be enrolled on equipment that verifies identity by means of a personal characteristic.

(b) Procedures that call for certain administrative approvals prior to removal of SNM from a vault or other material access area.(12)

(c) Methods used in qualifying guard forces and training them in the procedures needed to detect, delay, deter and/or neutralize a threat to the specific facility.(2)

(d) Procedures established to obtain support of a local law enforcement authority when required.

How well these procedures are followed and whether or not they are, as established, sufficient to provide effective security are the two major concerns to be evaluated in arriving at an MOE for these procedures. Of course, all such administrative procedures that may have a significant bearing on physical security system/element effectiveness must be considered.

Operational Procedures

Operational procedures employed by guard forces and others concerned with security at a facility are usually much more extensive and often more critical than are administrative procedures. However, the same concerns of sufficiency of and adherence to the procedures mentioned above are important here as well. Several examples of such operational procedures are:

(a) Those used by guards in patrolling the perimeter of a protected area.

(b) Those used in controlling access to a secure area (protected, vital, material access), particularly when the procedure is manual (badge comparison or exchange badge methods, for example).

(c) Those used for alarm assessment in which guards at the central alarm monitoring station or on patrol determine the cause of an alarm or that it is a false alarm.

(d) Those used to protect a perimeter or other area under emergency conditions when electronic sensors are unavailable or inoperable.

(e) Those used in securing vital and material access areas during fires or similar situations requiring emergency evacuation.

(f) Those used by guards or local law enforcement authority personnel in responding to intruder alarms.

(g) Those used by guards to search for contraband (explosives, incendiary devices, SNM, weapons) when appropriate sensors are unavailable or in conjunction with such sensors when they are employed.

(h) Those used to communicate with other guard forces or LLEA forces when primary communication links have been disrupted.

SUMMARY

For all of the above parameters, data will be obtained by inspectors in the field on individual items of physical protection equipment, barrier structures or guard performance and procedures. The data will be based either on quantified subjective judgments using checklists (to be prepared as part of the program to develop this methodology for measuring levels of effectiveness) or on the analysis of measurements made by the inspectors and by the

licensee. Some information cannot be measured in the field but is needed to arrive at an effectiveness level (e.g., error rate of coded card devices). In these cases generic inputs from the basic predictive model selected for use by NRC should be employed when available. An alternative would be to include the parameters as variables, appropriately weighted, in the MOE algorithm The contribution of that parameter should then be established, and the actual effectiveness of any system element may be indicated as a function of each variable parameter. Eventually studies would have to be initiated to determine how to evaluate or measure all significant parameters which have not been appropriately characterized.

Although many of the parameters bearing on equipment/procedure/system effectiveness have been mentioned above, these are not all-inclusive lists. As more information is developed about the system elements and the importance of certain data to computation of an MOE, those additional parameters identified should be included in the algorithms used.

SECTION IV

THREAT CONSIDERATIONS AND ADVERSARY CHARACTERISTICS

Several levels of threat can be considered in determining effectiveness, and an MOE should be established for each type of threat hypothesized. A threat is characterized by the number of adversaries, their physical and mental characteristics, their level of knowledge about the facility being protected and its physical protection system, the tools or penetration aids at their disposal, and the extent of inside assistance, if any. At least three threats covering the range of potential adversary characteristics should be selected as the basis for measuring system element, or entire system, effectiveness.[13,14] Although the specific threats to be used should be approved by NRC as being the most appropriate, there are several generalized threats defined in 10 CFR 73.55 and in ANSI N18.17-1973 which is cited by that CFR (although not specifically with regard to threat characteristics). No comparable threat is given in 10 CFR 73.50.

The threats characterized in 10 CFR 73.55 are:

(1) A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (i) well-trained (including military training and skills) and dedicated individuals, (ii) inside assistance which may include a knowledgeable individual who attempts to participate in both a passive role (e.g., provide information) and an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), (iii) suitable weapons, up to and including

hand-held automatic weapons equipped with silencers and having effective long range [illegible] (iv) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or otherwise destroying the reactor integrity, and

(2) An internal threat of an insider, including an employee (in any position).

Note that the number of individuals involved in a determined external assault is not specific, but could consist of six, ten or even more people (a recent incident in Washington, D.C., involved the coordinated efforts of 12 armed and knowledgeable adversaries in taking over three unguarded buildings). A maximum level threat could involve 25 individuals plus reserves[14]; however the MOE to be developed should give prime consideration to an attack of less than this paramilitary size force. Several different values may be arrived at, using appropriate methodologies, depending upon whether the attempt at penetration was by direct assault, by stealth or by deceit. However, lesser level threats should also be considered so that a range of capabilities can be determined for any specific facility. For example, the effectiveness of a physical protection system (or one of its elements) may be only 85% (or 0.85) for the maximum level threat postulated, but may increase to almost 100% when certain attributes of the adversary are reduced, such as fewer adversaries, less knowledgeable, lower level of weapons effectiveness, and with less or no inside assistance. For attacks by stealth or deceit, the knowledge that the adversary possesses and the availability to him of suitable tools become more important and must be weighted accordingly, while for a determined assault, the types of weapons and explosives being used would be more important. In addition, because different sensor types will detect different adversary physical characteristics, these must be well-defined in characterizing the threat.

Another approach that can be taken for higher level threats is the assumption that the vulnerabilities and limitations of specific equipment and structures at a site are known to the adversary, and that if a technique is available to the adversary for taking advantage of these factors, that technique will be used. Any such known vulnerability that has not been compensated for in the actual installation as determined by the inspector should be included in the MOE. This could also be varied as a function of the level of knowledge an adversary is assumed to possess. An MOE that can be varied as a function of adversary attributes assumed would be most useful.

It must be recognized that the adversary characteristics selected in developing each of the several MOE's discussed earlier will be, at best, educated guesses based on studies performed by others[12,14,15] and by those in a position at NRC to make that decision. However, the uncertainty resulting from this selection process is mitigated by the use of a range of threats with the expectation that the actual adversary, if indeed any individual or group would attempt sabotage of a facility or theft/diversion of SNM, will lie somewhere within this range. As a result, the level of effectiveness of the system or its individual elements computed for each selected threat should bracket the "true" effectiveness that would be achieved under actual conditions.

In summary, then, the methodology to be developed for establishing specific MOE's and using them to determine levels of effectiveness must consider specific adversary characteristics and adversary actions. These will directly affect computation of such parameters as time delays provided by or deterrent qualities of barrier structures, the probability of detection provided by sensors, the detection/deterrent levels afforded by access/entry control systems, the degree

of protection afforded by alarm signalling or other communications networks as a function of the sophistication of their line supervision capabilities, the effectiveness of guard and response forces and similar considerations. All of these are critical to the computation of the actual level of effectiveness achieved at a specific facility licensed by the NRC.

APPENDIX I

TYPICAL SYSTEM CONFIGURATIONS

Research Facilities

The protection afforded to research facilities will be a direct function of the quantity of SNM that they handle. Several typical physical protection configurations are listed below.

Level of Protection

1. Minimum
   a) Barrier structures are walls and locked doors
   b) Guard at entrance
   c) Picture badge identification
   d) Telephone communications to local law enforcement authority (LLEA)

2. Low Level
   a) Barrier structures are walls and locked doors
   b) Guard at entrance
   c) Picture badge identification
   d) Doors and windows alarmed
   e) Hand-held metal detectors
   f) Hand-held health physics device search for SNM
   g) Telephone communications to local law enforcement authority (LLEA)

3. Moderate Level
   a) Barrier structures are reinforced walls
   b) Doors and windows locked and alarmed
   c) Continuously manned central alarm monitoring station
   d) Identification by badge using split screen TV and TV monitoring of entrance
   e) Walk-through and hand-held metal, explosive and SNM detectors as appropriate
   f) Alarm assessment by guard response (<5 min.)
   g) Telephone communications to local law enforcement authority (LLEA) and two-way portable radio communications between guards

4. High Level
   a) Barrier structures are reinforced walls
   b) Doors and windows locked and alarmed
   c) Identification/access control by code entered on keyboard and coded card

d) Walk-through and hand-held metal, explosive and SNM detectors as appropriate
e) Continuously manned central alarm monitoring station
f) Secondary alarm monitoring station
g) Alarm assessment by CCTV
h) Low level line supervision (detect cuts and shorts only)
i) Telephone communications to local law enforcement authority (LLEA) with backup radio communications
j) Two-way portable radio communications between guards

Power Reactors

The following configurations represent various levels of protection that may be afforded to nuclear power reactors. The minimum level should meet all requirements of 10 CFR 73.55.

Level of Protection

5. Minimum
   a) Perimeter fence around protected area
   b) Guard patrol (every 1-2 hours) - periodic
   c) Guard at entrance to protected area
   d) Picture badge identification for entry/access control
   e) Vital areas separately protected by fence, walls and locked doors and windows
   f) Magnetic switch alarms (or equivalent) on doors and windows to/from vital areas
   g) Central alarm monitoring station within protected area and treated as a vital area
   h) Secondary alarm monitoring station provided
   i) Alarm assessment by direct visual assessment
   j) Guard response to threat $\leq$5 min.
   k) Telephone communications to local law enforcement authority (LLEA) with backup radio communications
   l) Two-way portable radio communications between guards

6. Low Level
   a) Perimeter fence around protected area
   b) Guard patrol (every 1-2 hours) - periodic
   c) Guard at entrance to protected area
   d) Picture badge identification for entry/access control
   e) Vital areas separately protected by fence, walls and locked doors and windows
   f) Magnetic switch alarms (or equivalent) on doors and windows to/from vital areas
   g) Hand-held metal detectors used
   h) Central alarm monitoring station within protected area and treated as a vital area
   i) Secondary alarm monitoring station provided

j) Alarm assessment by direct visual assessment augmented by CCTV around perimeter
k) Guard response to threat ≤5 min.
l) Telephone communications to local law enforcement authority (LLEA) with backup radio communications
m) Two-way portable radio communications between guards

7. Moderate Level
a) Perimeter fence around protected area
b) Perimeter sensor alarm system of moderate capability (e.g., fence perturbation detection sensors, simple IR beams; devices that protect against bridging of fence, digging under fence, or other simple countermeasures)
c) Guard patrol on irregular schedule of 5 min. to 1 hr.
d) Identification for entry/access control by exchange badge system, or by split screen TV (comparing badge and individual) with entrance under TV surveillance
e) Vital areas are separately protected by fences and, when possible, buildings having reinforced walls, roofs and floors; doors are reinforced in protective frames with inaccessible hinges; buildings have either no windows or non-opening windows protected by special glazing materials and/or grilles
f) Doors are locked with at least 11/16-inch dead bolt lock and security type key (non-pickable lock), and have balanced magnetic switch alarms (or equivalent)
g) Access to vital areas monitored by guards
h) Vital areas have volume intrusion detection alarms (e.g., IR, ultrasonic or microwave)
i) Central alarm monitoring station within protected area and treated as a vital area
j) Secondary alarm monitoring station provided
k) Perimeter alarm assessment augmented by CCTV, preferably fixed mount
l) Walk-through and hand-held metal and explosive detectors as appropriate
m) Guard response ≤5 min.
n) Low level line supervision (detect open (cut) and short circuits)
o) Telephone communications to local law enforcement authority (LLEA) with backup radio communications
p) Two-way portable radio communications between guards

8. High Level
a) Perimeter fence around protected area
b) Perimeter sensor alarm system of high level capability (e.g., buried line magnetic/seismic detectors, microwave sensors with overlapping patterns, E-field

type sensors, etc.). Sensors are more reliable and less susceptible to countermeasures or circumvention

c) Guard patrol on irregular schedule of 5 min. to 1 hr.
d) Identification for entry/access control for both protected and vital areas by keyed in code number and coded card/device with entrance under TV surveillance to detect tailgating, vandalism and forcible entry. Note that doors do not have key locks, only alarmed crash bars to permit emergency exit from vital areas and protected area
e) Vital areas are separately protected by fences and, when possible, buildings having reinforced walls, roofs and floors; doors are reinforced in protective frames with inaccessible hinges; buildings have either no windows or non-opening windows protected by special glazing materials and/or grilles
f) Doors are locked with at least 11/16-inch dead bolt lock and security type key (non-pickable lock), and have balanced magnetic switch alarms (or equivalent)
g) Vital areas have volume intrusion detection alarms (e.g., IR, ultrasonic or microwave)
h) Central alarm monitoring station within protected area and treated as a vital area
i) Secondary alarm monitoring station provided
j) Perimeter and interior area alarm assessment augmented by CCTV (preferably fixed mount)
k) Walk-through and hand-held metal and explosive detectors as appropriate
l) Guard response to any protected area < min.
m) Line supervision protects against cuts, shorts and most bridging by using coded messages and polling or "hand-shake" techniques
n) Telephone communications to local law enforcement authority (LLEA) with backup radio communications. Automatic transmission of prerecorded alert message to LLEA and remote response forces
o) Two-way portable radio communications between guards

9. Very High Level
   a) Perimeter fence around protected area
   b) Two types of high level capability perimeter sensor alarm system used in parallel, having complementary strengths and vulnerabilities
   c) Identification for entry/access control for protected area by keyed in code number and coded card/device. Identification for entry/access control for vital areas by personal characteristic verification (hand-writing, fingerprint, etc.). In both cases a control element (man-trap) isused which employs appropriate

sensors and TV surveillance components to prevent/discourage tailgating. No key locks on doors. Alarmed crash bars to permit emergency exit from control element, protected area or vital areas

d) Guard patrol on irregular schedule of 5 min. to 1 hr.
e) Vital areas are separately protected by fences and, when possible, buildings having reinforced walls, roofs and floors; doors are reinforced in protective frames with inaccessible hinges; buildings have either no windows or non-opening windows protected by special glazing materials and/or grilles
f) Doors are locked with at least 11/16-inch dead bolt lock and security type key (non-pickable lock), and have balanced magnetic switch alarms (or equivalent)
g) Vital areas have volume intrusion detection alarms (e.g., IR, ultrasonic or microwave)
h) Central alarm monitoring station within protected area and treated as a vital area
i) Secondary alarm monitoring station provided
j) Perimeter and interior area alarm assessment augmented by CCTV (preferably fixed mount)
k) Walk-through and hand-held metal and explosives detectors as appropriate
l) Guard response to any protected area <2 min.
m) Line supervision protects against cuts, shorts and most bridging by using coded messages and polling or "handshake" techniques
n) Telephone communications to local law enforcement authority (LLEA) with backup radio communications. Automatic transmission of prerecorded alert message to LLEA and remote response forces
o) Two-way portable radio communications between guards

SNM Processing Facility

Other fuel cycle facilities handling, producing or processing special nuclear materials as defined in 10 CFR 70 require protection at higher levels, in general (see 10 CFR 73.50), as well as protection of material access areas.

Level of Protection

10. Minimum
a) Perimeter fence around protected area
b) Perimeter sensor alarm system of moderate capability (e.g., fence perturbation detection sensors, simple IR beams; devices that protect against bridging of fence, digging under fence, or other simple countermeasures)

c) Guard patrol on irregular schedule of 5 min. to 1 hr.
d) Identification for entry/access control to protected area by exchange badge system, or by split screen TV (comparing badge and individual) with entrance under TV surveillance
e) Vital areas are separately protected by fences and, when possible, buildings having reinforced walls, roofs and floors; doors are reinforced in protective frames with inaccessible hinges; buildings have either no windows or non-opening windows protected by special glazing materials and/or grilles
f) Material access areas are within vital area buildings having reinforced walls, roofs and floors. SNM stored in vaults
g) Doors are locked with at least 11/16-inch dead bolt lock and security type key (non-pickable lock), and have balanced magnetic switch alarms (or equivalent)
h) Access to vital and material access areas monitored by guards
i) Vital areas have volume intrusion detection alarms (e.g., IR, ultrasonic or microwave)
j) Material access areas under constant observation by personnel
k) Central alarm monitoring station within protected area and treated as a vital area
l) Secondary alarm monitoring station provided
m) Perimeter alarm assessment augmented by CCTV (preferably fixed mount)
n) Walk-through and hand-held metal, explosive and SNM detectors used as appropriate
o) Guard response $\leq$5 min.
p) Low level line supervision (detect open (cut) and short circuits)
q) Telephone communications to local law enforcement authority (LLEA) with backup radio communications
r) Two-way portable radio communications between guards

11. Moderate Level
a) Perimeter fence around protected area
b) Perimeter sensor alarm system of high level capability (e.g., buried line magnetic/seismic detectors, microwave sensors with overlapping patterns, E-field type sensors, etc.). Sensors are more reliable and less susceptible to countermeasures or circumvention
c) Guard patrol on irregular schedule of 5 min. to 1 hr.
d) Identification for entry/access control for both protected and vital areas by keyed in code number and coded card/device with entrance under TV surveillance

to detect tailgating, vandalism and forcible entry. Note that doors do not have key locks, only alarmed crash bars to permit emergency exit from vital areas and protected area

e) Identification for entry/access to material access areas monitored by guards either with exchange badge system or use of keyed in code numbers and coded cards/ devices. Doors as above

f) Vital areas are separately protected by fences and, when possible, buildings having reinforced walls, roofs and floors; doors are reinforced in protective frames with inaccessible hinges; buildings have either no windows or non-opening windows protected by special glazing materials and/or grilles

g) Material access areas are within vital area buildings having reinforced walls, roofs and floors. SNM stored in vaults

h) Doors are locked with at least 11/16-inch dead bolt lock and security type key (non-pickable lock), and have balanced magnetic switch alarms (or equivalent)

i) Vital areas have volume intrusion detection alarms (e.g., IR, ultrasonic or microwave)

j) Material access areas under constant observation by personnel and CCTV

k) Central alarm monitoring station with in protected area and treated as a vital area

l) Secondary alarm monitoring station provided

m) Perimeter and interior area alarm assessment augmented by CCTV (preferably fixed mount)

n) Walk-through and hand held metal, explosives and SNM detectors used as appropriate

o) Guard response to any protected, vital or material access area <2 min.

p) Line supervision protects against cuts, shorts and most bridging by using coded messages and polling or "handshake" techniques

q) Telephone communications to local law enforcement authority (LLEA) with backup radio communications. Automatic transmission of prerecorded alert message to LLEA and remote response forces

r) Two-way portable radio communications between guards

12. High Level

a) Perimeter fence around protected area

b) Two types of high level capability perimeter sensor alarm system used in parallel, having complementary strengths and vulnerabilities

c) Identification for entry/access control for protected area by keyed in code number and coded card/device. Identification for entry/access control for vital/material access areas by personal characteristic verification (handwriting, fingerprint, etc.). In both cases a control element (man-trap) is used which employs appropriate sensors and TV surveillance components to prevent/discourage tailgating. No key locks on doors. Alarmed crash bars to permit emergency exit from control element, protected area or vital/material access area
d) Guard patrol on irregular schedule of 5 min. to 1 hr.
e) Vital areas are separately protected by fences and, when possible, buildings having reinforced walls, roofs and floors; doors are reinforced in protective frames with inaccessible hinges; buildings have either no windows or non-opening windows protected by special glazing materials and/or grilles
f) Material access areas are within vital area buildings having reinforced walls, roofs and floors. SNM stored in vaults
g) Material access area roofs, walls and floors alarmed with imbedded grid sensors. Capacitance, IR or other point and volume detectors used as appropriate
h) Doors are locked with at least 11/16-inch dead bolt lock and security type key (non-pickable lock), and have balanced magnetic switch alarms (or equivalent)
i) Vital areas have volume intrusion detection alarms (e.g., IR, ultrasonic or microwave)
j) Central alarm monitoring station within protected area and treated as a vital area
k) Secondary alarm monitoring station provided
l) Material access areas under constant observation by personnel and CCTV
m) Perimeter and interior area alarm assessment augmented by CCTV (preferably fixed mount)
n) Walk-through and hand-held metal, explosive and SNM detectors used as appropriate
o) Guard response to any protected, vital or material access area <2 min.
p) Line supervision protects against cuts, shorts and most bridging by using coded messages and polling or "handshake" techniques
q) Telephone communications to local law enforcement authority (LLEA) with backup radio communications. Automatic transmission of prerecorded alert message to LLEA and remote response forces

r) Two-way portable radio communications between guards

APPENDIX II

REFERENCES

1. Code of Federal Regulations, Title 10 (10 CFR); Energy; Parts 0 to 199; January 1977

2. U. S. Nuclear Regulatory Commission Regulatory Guides

   1.17 Protection of Nuclear Power Plants Against Industrial Sabotage (6/73)

   5.7 Control of Personnel Access to Protected Areas, Vital Areas, and Material Access Areas (6/73)

   5.12 General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials (11/73)

   5.14 Visual Surveillance of Individuals in Material Access Areas (11/73)

   5.20 Training, Equipping and Qualifying of Guards and Watchmen (11/74)

   5.27 Special Nuclear Material Doorway Monitors (6/74)

   5.43 Plant Security Force Duties (1/75)

   5.44 Perimeter Intrusion Alarm Systems (Revision 1, 6/76)

3. NUREG-0141 (RAD-TR-5000-002), An Assessment of Some Safeguards Evaluation Techniques, Final Report; Gref, L. G., Rosengren, J. W.; prepared by R&D Associates, Arlington, VA 22209 for the United States Nuclear Regulatory Commission; February 1977

4. SAND76-0428, Safeguards Systems Effectiveness Modeling; Boozer, D. D., et. al.; Sandia Laboratories; September 1976

5. NUREG-760145 (SAND76-0500), The "EASI" Approach to Physical Security Evaluation; Bennett, H. A.; Sandia Laboratories; January 1977

6. RADC-TR-72-26 (LMSC-D053773), Capability Measures for System Effectiveness; Chop, A. I.; prepared by Lockheed Missiles and Space Co., Sunnyvale, CA; February 1972

7. NWC TP 5298, System Analysis Guide; prepared by Dunlap and Associates, Inc. for Naval Weapons Center, China Lake, CA; January 1972

8. Typical Pitfalls of Effectiveness Analysis; Fleck, J. J.; General Electric Co., Schenectady, NY; March 1970

9. NUREG-0273 (MTR-03444), Guide for the Evaluation of Physical Protection Equipment; The MITRE Corporation, Bedford, MA; July 1977

10. NUREG-0271 (MTR-03458), Final Report: Study of Physical Protection Equipment; Haberman, W.; The MITRE Corporation, Bedford, MA; June 1977

11. NUREG-0272 (MTR-03445), Catalog of Physical Protection Equipment; The MITRE Corporation, Bedford, MA; July 1977

12. NUREG-0156, The White-Collar Challenge to Nuclear Safeguards; prepared by Battelle Human Affairs Research Centers, Seattle, WA 98105 for the United States Nuclear Regulatory Commission; January 1977

13. SAND75-0391, Physical Security Systems Effectiveness Evaluation - A Status Report; Todd, J. L., Nickell, W. C.; Sandia Laboratories; July 1975

14. SAND75-0627, Adversary Characterization for Security System Evaluation; Suber, L. A.; Sandia Laboratories; April 1976

15. MTR-7022, The Threat to Licensed Nuclear Facilities; Burnham, S., et. al.; The MITRE Corporation; September 1975

APPENDIX III

BIBLIOGRAPHY

NUREG-75/014 WASH-1400	Reactor Safety Study--An Assessment of Risks in U. S. Commercial Nuclear Power Plants; Executive Summary; United States Nuclear Regulatory Commission; October 1975
NUREG-0095 ERDA77-34	Joint ERDA-NRC Task Force on Safeguards (U), Final Report; United States Nuclear Regulatory Commission; July 1976
WP-5471	Measures of Effectiveness for the Airfield Denial System Using ADTAGS/ADTAMS; Honda, L. N.; The MITRE Corporation; August 1973
SAND75-0504	Safety and Security of Nuclear Power Reactors to Acts of Sabotage; Sandia Laboratories; March 1976
SAND75-6061	Fixed-Site Physical Protection Systems Modeling; Chapman, L. D.; Sandia Laboratories; December 1975
SAND75-6136	Statement of Dr. Orval E. Jones, Director Nuclear Security Systems, before the Assembly Committee on Resources, Land Use, and Energy of the California Legislature; Sandia Laboratories; November 1975
SAND75-6159	Effectiveness Evaluation of Alternative Fixed-Site Safeguard Security Systems; Chapman, L. D.; Sandia Laboratories; July 1976
SAND76-0637 NUREG-0144	Summary Report of Workshop on Sabotage Protection in Nuclear Power Plant Design; Sandia Laboratories; February 1977
SAND76-5143	Safeguards for the Physical Protection of Nuclear Materials and Facilities, Statement submitted to the U. S. Senate Committee on Government Operations; Jones, O. E.; Sandia Laboratories; January 1976
SAND76-5388	Advanced Physical Protection Systems for Facilities and Transportation; Sandia Laboratories; Jones, O. E.
SAND76-5519	Nuclear Safeguards; Ney, J. F.; Sandia Laboratories; June 1976
SAND76-5648	The Design of Integrated Safeguards Systems for Nuclear Facilities; deMontmollin, J. M., Walton, R. B.; Sandia Laboratories; 1976

ERDA-7 Societal Risk Approach to Safeguards Design and Evaluation; Energy Research and Development Administration; June 1975

DISTRIBUTION LIST

INTERNAL

D-80

F. W. Hopkins
J. H. Phillips
A. J. Roberts

D-81

L. I. Egelson
J. B. Frazer
A. J. Graff
W. Haberman (5)
G. A. Klein
J. W. Myers
S. M. Newman
W. L. Parlee
G. O. Sauermann

EXTERNAL

U. S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Division of Safeguards, Fuel Cycle and Environmental Research
Washington, D.C. 20555

H. M. Hawkins (20)