SANDIA REPORT
SAND2007-5591
Unlimited Release
Printed September 2007

Nuclear Power Plant Security Assessment Technical Manual

D. W. Whitehead
C. S. Potter
S. L. O'Connor

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-5591
Unlimited Release
Printed September 2007

Nuclear Power Plant Security Assessment Technical Manual

D. W. Whitehead
Security Risk Assessment Department

C. S. Potter
Active Response and Denial Department

S. L. O'Connor
Organizational Learning, Conference Planning, and Communications Department
P.O. Box 5800
Albuquerque, NM 87185-0758

Abstract

This report (*Nuclear Power Plant Security Assessment Technical Manual*) is a revision to NUREG/CR-1345 (*Nuclear Power Plant Design Concepts for Sabotage Protection*) that was published in January 1981. It provides conceptual and specific technical guidance for U.S. Nuclear Regulatory Commission nuclear power plant design certification and combined operating license applicants as they:

- develop the layout of a facility (i.e., how buildings are arranged on the site property and how they are arranged internally) to enhance protection against sabotage and facilitate the use of physical security features,
- design the physical protection system to be used at the facility, and
- analyze the effectiveness of the PPS against the design basis threat.

It should be used as a technical manual in conjunction with the *Nuclear Power Plant Security Assessment Format and Content Guide*. The opportunity to optimize physical protection in the design of a nuclear power plant is obtained when an applicant utilizes both documents when performing a security assessment.

This document provides a set of best practices that incorporates knowledge gained from more than 30 years of physical protection system design and evaluation activities at Sandia National Laboratories and insights derived from U.S. Nuclear Regulatory Commission technical staff into a manual that describes a development and analysis process of physical protection systems suitable for future nuclear power

plants. In addition, selected security system technologies that may be used in a physical protection system are discussed.

The scope of this document is limited to the identification of a set of best practices associated with the design and evaluation of physical security at future nuclear power plants *in general*. As such, it does not provide specific recommendations for the design and evaluation of physical security for any specific reactor design. These best practices should be applicable to the design and evaluation of physical security for *all* future plants.

Note that the original NUREG/CR-1345 remains valid for many light water reactor designs.

While the focus of this document is on new plants, existing nuclear power plants and nuclear material facilities may be able to apply these best practices and security system technologies when upgrading or modifying their physical protection systems.

ACKNOWLEDGEMENTS

The authors thank all of the many contributors to Section 5. Without their help this section would have taken significantly longer to produce. To John Darby of Sandia National Laboratories, thank you for your technical review. To Betty Biringer of Sandia National Laboratories, thanks for all your support. Finally, we would like to thank Albert Tardiff of the U.S. Nuclear Regulatory Commission for his guidance throughout this project. His guidance helped make this document a better product.

Contents

Figures

Tables

NOMENCLATURE

3DVMD	Three-Dimensional Video Motion Detection
AC&D	alarm communication and display
ACAV II	Advanced Concept Armored Vehicle II
ACP	access control point
ADKBS	Access Delay Knowledge-Based System
ADS	Active Denial System
ASD	Adversary Sequence Diagram
ASSESS	Analytic System and Software for Evaluating Safeguards and Security
ATLAS	Adversary Time-Line Analysis System
CCTV	closed circuit television
CDP	critical detection point
CPU	central processing unit
CS	ortho-chlorobenzylidene malononitrile
CSR	Counter-Sniper ROWS
CTMC	continuous time Markov chain
DBT	design basis threat
DoD	Department of Defense
DOE	Department of Energy
EASI	Estimate of Adversary Sequence Interruption
EDS	explosives detection system
FOF	force on force
GBR	ground-based radar
GSR	ground surveillance radar
GUI	graphical user interface
IDS	Intrusion Detection System
IT	intelligent targeting
JCATS	Joint Conflict and Tactical Simulation
MBADS	Munitions-Based Access Denial System
MOX	mixed oxide
NAR	nuisance alarm rate
NRC	U.S. Nuclear Regulatory Commission
OC	oleoresin capsicum
PDP	practical detection point
PE	protection element
PIDAS	Perimeter Intrusion Detection and Assessment System
PPS	physical protection system
ROWS	Remotely Operated Weapon Systems
SAVI	Systematic Analysis of Vulnerability to Intrusion
SEDS	System Enable Disable Switch
SNL	Sandia National Laboratories
TacNet	Tactical Network
VPED	Virtual Presence and Extended Defense

1. INTRODUCTION

1.1 Background

The U.S. Nuclear Regulatory Commission (NRC) has received an increase in design certification applications for nuclear power plants and anticipates several others by 2008. The NRC has also been notified of the intent to submit ten or more combined license applications between FY2007 and FY2008. As such there is renewed interest to update and revise NUREG/CR-1345, which was originally published in 1981. This version of the revised NUREG/CR-1345 is titled *Nuclear Power Plant Security Assessment Technical Manual*.

This manual should be used when design certification or combined license applicants perform a security assessment and should be used in conjunction with the *Nuclear Power Plant Security Assessment Format and Content Guide* [Ref. 1].

The NRC staff requested the revision employ a more global rather than design-specific approach (as was done in the original NUREG/CR) such that the revised NUREG/CR may be applicable to the many various reactor designs being presented, including future Generation IV designs.

1.2 Purpose

The purpose of this document is to provide conceptual and specific technical guidance[1] for nuclear power plant design certification and combined operating license applicants as they:

- develop the layout of a facility (i.e., how buildings are arranged on the site property and how they are arranged internally) to enhance protection against sabotage and facilitate use of physical security features
- design the physical protection system (PPS) to be used at the facility
- analyze the effectiveness of the PPS against the design basis threat

It should be used as a technical manual in conjunction with Reference 1. The opportunity to optimize physical protection in the design of a nuclear power plant is obtained when an applicant utilizes both documents when performing a security assessment.

1.3 Objectives

The objective of this guidance document is to incorporate knowledge gained from more than 30 years of PPS design and evaluation activities at Sandia National Laboratories (SNL) and insights derived from the NRC technical staff into a set of best practices for application to the development and analysis of physical protection systems for future nuclear power plants.

The document has been written in plain English and explanatory text to the greatest extent possible to allow those unfamiliar with physical protection to utilize the information presented.

[1]The authors recognize that while the guidance provided in this document is based upon knowledge gleaned from past experiences and analyses, it may not prove infallible for all possible future events. Nevertheless, the authors believe the guidance presented here represents the best information available at this time.

1.4 Scope

The scope of this project is limited to the identification of a set of best practices associated with the design and evaluation of physical security at future nuclear power plants *in general*. As such, it does not provide specific recommendations for the design and evaluation of physical security for any specific reactor design. These best practices should be applicable to the design and evaluation of physical security for *all* future plants.

Existing nuclear power plants and certain nuclear material facilities may be able to apply these best practices when upgrading or modifying their physical protection systems.

1.5 Report Organization

Chapter 1 provides an introduction to the report. Background material is presented in Section 1.1, and the purpose, objectives, and scope are presented in Sections 1.2, 1.3, and 1.4, respectively. Chapter 2 provides a high-level overview of the recommended approach for designing an effective PPS and analyzing its performance. Chapter 3 provides a brief description of a representative set of currently available analytical tools that can be used in a security system performance assessment. Chapter 4 provides a compilation of high-level and conceptual guidance (i.e., best practices) distilled from more than 30 years of work in the area of physical security system design. These best practices should be considered during the design of a physical security system. Chapter 5 provides a brief description of a selected set of security system technologies that a nuclear power plant design team might consider during the design of the plant and its physical security system. Chapter 6 provides a summary of the observations and insights from the NUREG/CR-1345 report that are appropriate for this document (i.e., observations and insights that are general in nature and not design specific). Chapter 7 concludes the report with a brief summary of the main points presented throughout the document.

2. DESIGN AND EVALUATION OF A PHYSICAL PROTECTION SYSTEM

This chapter presents a summary of the activities associated with the design and evaluation of a physical protection system (PPS). The purpose of this chapter is to *introduce* the major activities that must be accomplished during such a design and evaluation. For a more detailed, in-depth presentation on this topic (i.e., design and evaluation of a PPS) see *The Design and Evaluation of Physical Protection Systems* by Mary Lynn Garcia [Ref. 2]. Additionally, refer to another book by Garcia entitled *Vulnerability Assessment of Physical Protection Systems* [Ref. 3], which is an extension of the overall process and principles of physical protection systems presented in the first book to vulnerability assessment—identifying security system weaknesses that could potentially be exploited by malevolent human threats. These identified weaknesses are potential areas for improvement.

2.1 Overview

The design of an effective PPS includes identification of the PPS objectives, establishing the facility design, providing an initial design of a PPS, evaluation of the design, and a redesign or refinement of the system (if the system does not meet required protection objectives). Figure 2-1 is a pictorial representation of this process.

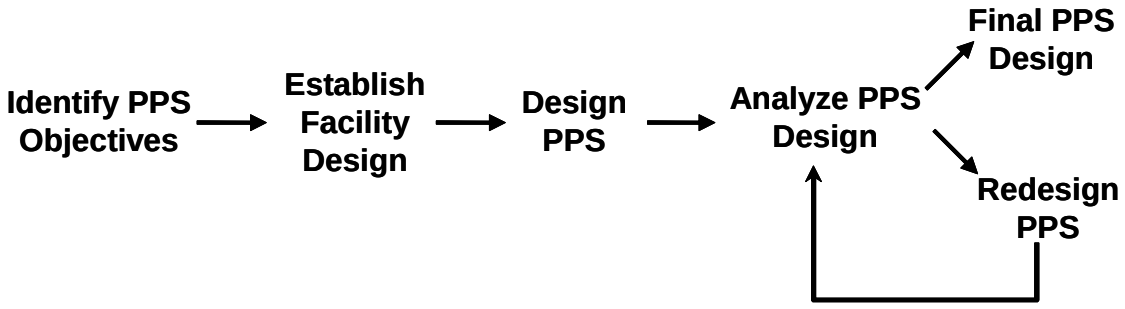

Figure 2-1. High-level description of a physical protection system design and evaluation process.

The designer should identify protection objectives for the facility from the applicable regulations. For U.S. nuclear power plants, protection objectives for the PPS are to provide high assurance of protection against significant core damage and sabotage (or theft[2]) of spent fuel against the design basis threat (DBT).[3] To establish the facility design the designer must begin by gathering information about facility operations and conditions, such as a comprehensive description of the facility, operating states, and the physical protection requirements. Next the designer should identify targets. Targets typically consist of equipment, personnel, and radioactive sources that, if damaged or destroyed, would result in unacceptable offsite consequences. The next step is to design the PPS. In designing the PPS, the designer must determine how best to

[2]For facilities that will use mixed oxide (MOX) fuel, the threat of theft or diversion of unirradiated MOX fuel assemblies must also be considered.

[3]The DBT defines (or describes) the following aspects about potential adversaries: class of adversary, adversary's capabilities, and range of adversary tactics.

combine such elements as fences, building structures, vaults, sensors, administrative procedures, communication devices, and protective force personnel to meet the objectives. Once a PPS is designed, it must be analyzed and evaluated to ensure it meets the physical protection objectives. Evaluation must allow for features working together to assure protection rather than regarding each feature separately. Due to the complexity of protection systems, an evaluation may require the application of modeling techniques. If the evaluation determines that PPS effectiveness[4] is unacceptable, then the initial system must be redesigned to correct vulnerabilities and a reevaluation conducted. This iterative process continues until the PPS effectiveness is determined to be acceptable. Figure 2-2 illustrates the activities associated with this design and evaluation process.

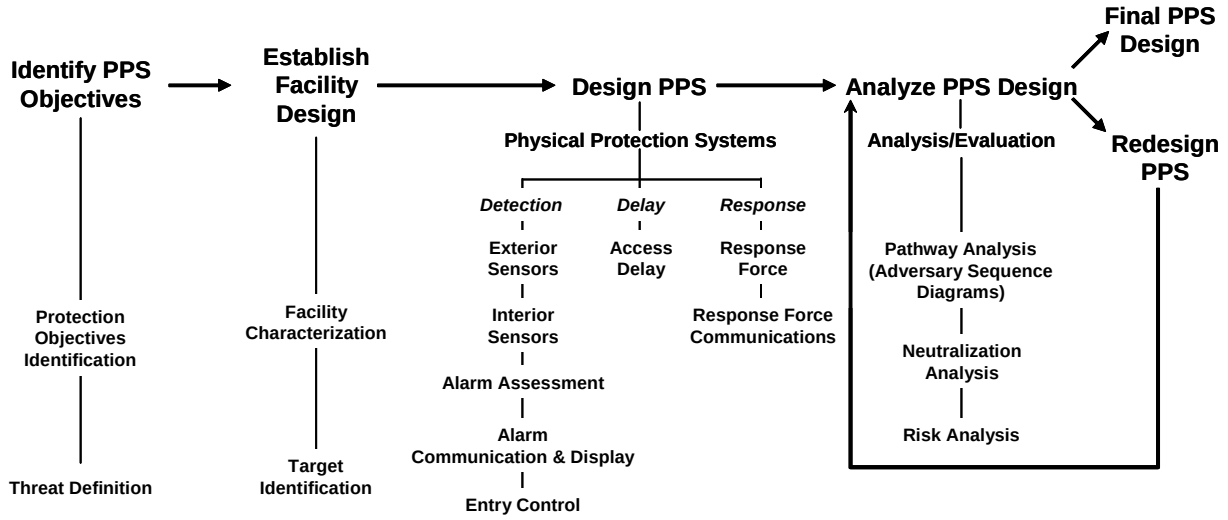

Figure 2-2. Activities associated with a physical protection system design and evaluation process.

This is a methodical approach in which the design and analysis of physical protection is conducted in an integrated fashion where all components of detection, delay, and response are properly weighted according to their contribution to the PPS as a whole. This approach can assist in minimizing the potential for wasting valuable resources on unnecessary protection while at the same time maximizing protection to the facility.

A simplified description of the recommended process of designing and analyzing a PPS is presented in the subsequent sections of this chapter.

2.2 Identify the PPS Objectives

The first major activity in the development of a PPS design, as shown in Figure 2-2, is *identify PPS objectives*. This activity involves two subtasks:

[4]The effectiveness of a PPS is determined as part of a malevolent-threat risk analysis. In this analysis risk is a function of the frequency of the threat (i.e., the DBT) occurrence, the probability that the PPS will fail to protect against the malevolent threat, and the consequences (i.e., the undesired events) associated with the failure of the PPS.

- threat definition
- protection objectives identification

These two subtasks are discussed in the following subsections.

2.2.1 Threat Definition

The threat definition will be defined by the DBT as provided by the U.S. Nuclear Regulatory Commission (NRC).[5]

The establishment of a threat definition typically considers the following three questions:

- What class of adversary is to be considered?
- What is the range of the adversary's tactics?
- What are the adversary's capabilities?

Adversaries can be separated into three classes:

- outsiders
- insiders
- outsiders in collusion with insiders

For each class of adversary, the full range of tactics (i.e., deceit, force, stealth, or any combination of these) is considered. Deceit is the attempted defeat of a security system by using false authorization and identification; force is the overt, forcible attempt to overcome a security system; and stealth is the attempt to defeat the detection system and enter the facility covertly.

Adversary capabilities include knowledge of the PPS, level of motivation, skills useful in carrying out the attack (e.g., knowledge of the safety systems), the speed with which the attack is carried out, and the ability to carry and use tools and weapons.

2.2.2 Protection Objectives Identification

Protection objectives are identified for each facility type from the applicable regulations. For U.S. nuclear power plants, protection objectives include high assurance of protection against significant core damage and sabotage of spent fuel. Prevention of theft of MOX fuel is also a protection objective for U.S. nuclear power plants that utilize MOX fuel assemblies. Protection objectives for NRC fuel fabrication licensees are prevention of theft of special nuclear material and radiological sabotage.

2.3 Establish Facility Design

The second major activity in the development of a PPS design, as shown in Figure 2-2, is *establish facility design*. This activity involves two subtasks:

[5] 10 CFR 73.1 addresses the DBT.

- facility characterization
- target identification

These two subtasks are discussed in the following subsections.

2.3.1 Facility Characterization

Establishing a facility's design requires the development of a thorough description of the facility itself (e.g., the location of the site boundary, location of buildings on the site, interior floor plans for the buildings, and access points for both the site and buildings), a thorough understanding of the various operations that take place at the facility, and knowledge of the different conditions that the facility will experience. This information can be obtained from sources such as facility design blueprints, process descriptions, safety analysis reports, probabilistic risk assessment reports, and environmental impact statements.[6] As with any complex facility that requires physical protection, compromises must be made among the three disciplines of safety, operations, and physical protection to ensure no one discipline is adversely affected by another.

2.3.2 Target Identification

To be able to develop adequate protection one must know what to protect. Protecting everything is neither possible nor practical. Thus effective security protects a minimum, yet a complete, set of items necessary to prevent the undesired consequences defined by the NRC. Undesirable consequences generally fall into two categories: those from theft of nuclear material and those from radiological sabotage. While both may have to be considered during the design and evaluation of a PPS, radiological sabotage typically represents the more limiting case for the PPS at a commercial nuclear power plant. This is because a radiological saboteur may need only to enter the site to destroy a target whereas for theft, the adversary must obtain special nuclear material and successfully exit the site. Therefore prevention of radiological sabotage, where an adversary must enter the site, is the focus for the remainder of this document.

For nuclear power plants the method of target identification includes starting with the probabilistic risk assessment (level 1) fault tree analysis and deriving target sets.

As defined in the proposed rule, 10 CFR 73.2, the term *Target Set* means the combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting, and/or core disruption) barring extraordinary action by plant operators. A target set with respect to spent fuel sabotage is draining of the spent fuel pool leaving the spent fuel uncovered for a period of time, allowing spent fuel heat-up and the associated potential for release of fission products.

A protection set is located in vital areas and is defined to be the set of locations and/or systems, structures, an components that if protected from access and/or damage ensure that the PPS pro-

[6]For new plants this information should be made available to the PPS designer as soon as possible so that the PPS designer can work with the plant designer to integrate security into the plant design. One simple example of this would be designing the equipment layout of the plant such that a set of equipment necessary to prevent undesired consequences is located in a single hardened structure with only one entrance/exit.

tection objectives are met (i.e., significant core damage, sabotage of spent fuel, and theft of un-irradiated MOX fuel assemblies do not occur).

Target set development is listed as a regulatory requirement within the proposed revision of 10 CFR 73.55. The NRC considers detailed consideration of target set development sensitive unclassified safeguards information. The NRC has developed guidance for target set development and it may be found in Appendix B of the *Nuclear Power Plant Security Assessment Format and Content Guide*.

It is also recommended that references [Ref. 4] and [Ref. 5] be reviewed before conducting target set development.

2.4 Design the Physical Protection System

The third major activity in the development of a PPS design, as shown in Figure 2-2, is *design PPS*. The objective of a PPS is to prevent the accomplishment of unauthorized overt or covert actions that result in radiological sabotage or theft of nuclear materials (i.e., the undesired events and subsequent consequences). The PPS must accomplish its objectives by either deterrence or a combination of detection, delay, and response.

Theft and sabotage may be prevented in two ways: by *deterring* the adversary or by *defeating* the adversary. Deterrence occurs by implementing a PPS that is seen by potential adversaries as too difficult to defeat; it makes the facility an unattractive target. In addition, legal ramifications associated with attacking a site may deter some adversaries, although not a determined one. The problem with deterrence is that it is impossible (or at least extremely difficult) to measure,[7] and therefore will not be discussed further. Defeating the adversary refers to the actions taken by the protective or response force to prevent an adversary from accomplishing his goal once he actually begins a malevolent action against a facility. There are three major functions that the PPS must perform. These include:

- detection
- delay
- response

These functions must be performed in a period of time that is less than the time required for the adversary to complete his tasks. Figure 2-3 shows the relationship between adversary task time and the time required for the PPS to do its job. The total time required for the adversary to accomplish his goal has been labeled Adversary Task Time. It is dependent upon the delay provided by the PPS. The adversary may begin his task at some time before the first alarm occurs (T_0). The adversary task time is shown by a dotted line before this point because delay is not effective before detection.[8] After that alarm, the alarm information must be reported and assessed to determine whether the alarm is valid. The time at which the alarm is assessed to be valid is

[7]It would be a mistake to assume because a system has not been challenged by an adversary that the effectiveness of the system has deterred such challenges.

[8]It is recognized that delay may be an effective contributor to *deterring* an adversary; however, for those cases where the adversary has not been deterred, delay before detection does not contribute to the effectiveness of the PPS.

labeled T_A, and at this time the location of the alarm must be communicated to the members of the response force. Further time is then required for the response force to respond in adequate numbers and with adequate equipment to interrupt and neutralize the adversary actions. The time at which the response force interrupts adversary actions is labeled T_I and adversary task completion time is labeled T_C. From an examination of this time line, it is clear that detection (i.e., T_0 and T_A) and response (i.e., T_I) should occur as early as possible; in other words, these events should be as far to the left on the time axis as possible.

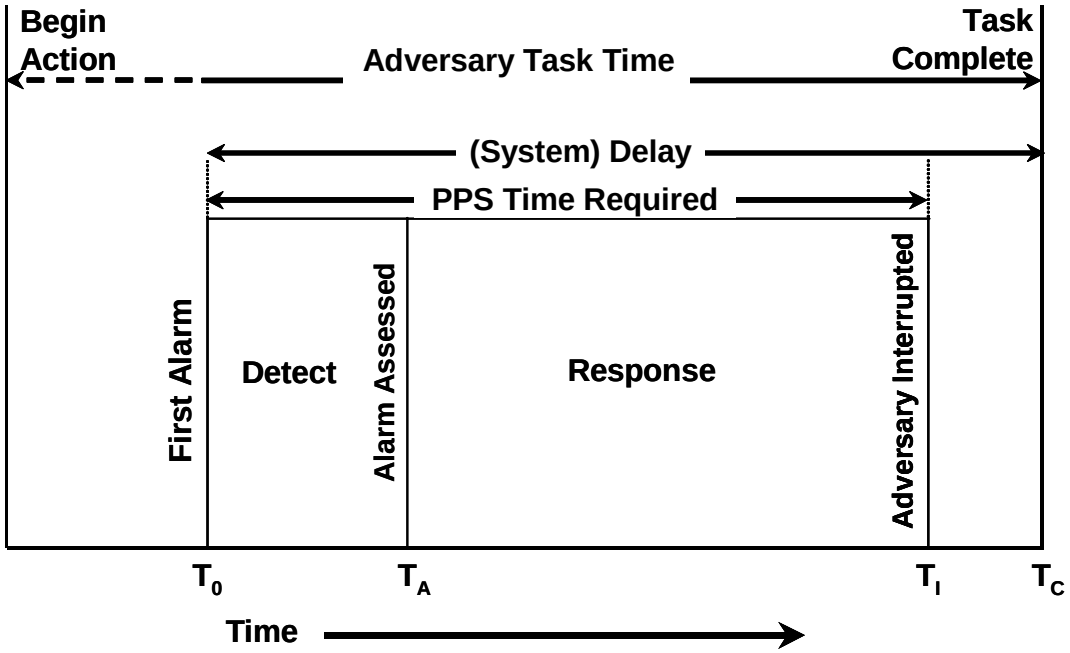

Figure 2-3. Interrelationship among physical protection system functions.

A brief discussion of each function is presented in the following subsection.

2.4.1 Physical Protection System Functions

2.4.1.1 Detection

Detection is the discovery of an adversary action. It includes sensing of covert or overt actions. To discover an adversary action, the following events must occur:

- A sensor[9] reacts to an abnormal occurrence and initiates an alarm.
- The information from the sensor and assessment subsystems is reported and displayed.
- A person assesses information and judges the alarm to be valid or invalid. If assessed to be a nuisance or false alarm,[10] a detection has not occurred. *Detection without assessment is not considered detection.*

[9]A sensor in this context could be a detection device or an individual.

[10]Regulatory Guide 5.44, Revision 3 defines a nuisance alarm as an alarm generated by an *identified input* [emphasis added] to a sensor or monitoring device that does not represent a safeguards threat. It defines a false alarm as an

These actions are depicted in Figure 2-4.

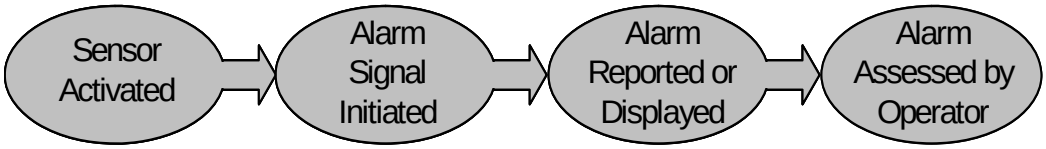

Figure 2-4. Actions comprising the detection function in a physical protection system.

The measure of effectiveness for the detection function is probability of detection, P_D, which is a function of the probability of sensing an adversary action, P_S, and the time required for an alarm signal to be generated, for the alarm to be reported, and for the alarm to be assessed. However an alarm is assessed it should be accomplished as soon after the alarm is generated to ensure adequate physical protection system effectiveness.

Detection can also be accomplished by the protective force or personnel. Guards at fixed posts or on patrol may serve a role in sensing (i.e., detecting) an intrusion; however the probability of detection associated with such activities is typically low. Personnel may contribute to detection of an insider action if the two-person rule is used in critical areas and the second person has a reliable means of signaling or communicating an alarm.

An effective assessment system provides two types of information associated with detection: information about whether the alarm is a valid, nuisance, or false alarm and details about the cause of the alarm (i.e., who they are, where they are, what they have, how many there are, and what they are doing).

2.4.1.1.1 External Sensors

The integration of individual sensors into a perimeter (i.e., external) sensor system must consider:

- specific design goals
- the effects of physical and environmental conditions
- the interaction of the perimeter system with a balanced and integrated PPS

Sensor performance is described by the following characteristics:

- probability of detection
- false and nuisance alarm rates
- vulnerability to defeat

The methods of classification of exterior sensors include:

---

alarm generated *without an apparent cause* [emphasis added]. Thus in both cases (i.e., nuisance and false alarms), detection has not occurred (i.e., no adversary detection has occurred).

- passive or active
- covert or visible
- line of sight or terrain following
- volumetric or line detection
- application (i.e., grouped by mode of application in the physical detection space)
  - buried-line
  - fence-associated
  - freestanding

An effective perimeter sensor system provides a continuous line of detection using multiple lines of complementary sensors located in an isolated clear zone. Topography, vegetation, wildlife, background noise, climate, weather, soil conditions, and pavement all affect the performance of exterior sensors. Using alarm priority schemes[11] can reduce the nuisance alarm rate. The designer of the perimeter sensor system must also consider its interaction with the video assessment system and the access delay system.

2.4.1.1.2 Interior Sensors

Interior intrusion sensors can be:

- active or passive
- covert or visible
- volumetric or line detectors

Their performance is discussed in terms of:

- probability of detection
- false and nuisance alarm rates
- vulnerability to defeat

The application classes include:

- boundary penetration sensors
- interior motion sensors
- proximity sensors

Various sensor technologies can be applied to achieve protection-in-depth:

[11]The nuisance alarm rate (NAR) can be significantly reduced by combining sensors with an AND gate if the nuisance alarms of the sensors are not correlated. A seismic sensor and an electric field sensor do not give correlated alarms, for example, because they respond to different things. If both are activated at about the same time, it is probable that they have detected an intrusion. A system can be designed to generate an alarm if two or more sensors are all activated within a preselected time interval (T). The nuisance alarm rate of the AND combination, NAR(AND), will be less than the nuisance alarm rate of each sensor. If the sensor outputs are uncorrelated and occur at a random rate that is much less than one output per selected time interval, T, then for two sensors, NAR(AND) = (T/60)(NAR1)(NAR2) where T is in minutes and NAR1 and NAR2 are nuisance alarms per hour for sensor 1 and sensor 2, respectively.

- at the boundary (e.g., of a building or a security area)
- within a room
- at the object to be protected

The designer of a good interior intrusion detection system considers the operational, physical, and environmental characteristics of the facility. Also, the designer should be familiar with:

- the sensors that are available
- how the sensors interact with the intruder and the environment
- the physical principles of operation for each sensor

The interior sensor system must support a balanced PPS.

2.4.1.1.3 Alarm Assessment

Assessment of perimeter alarms should be provided primarily by closed-circuit television (CCTV) coverage of each sensor sector displayed at a local alarm station monitored by security operators. Secondary or supplemental assessment may be accomplished by the protective force (guards) in towers and roving patrols.

Primary assessment of interior alarms can be accomplished by either CCTV displayed at a local alarm station or by guards only.

The assessment system is composed of:

- several cameras at remote sensor areas
- a display monitor at the local end
- various transmission, switching, and recording systems

The major components include:

- security operators who acknowledge and assess alarms
- the camera and lens to convert the image of the physical scene into an electrical signal
- the lighting system to illuminate the alarm location evenly with enough intensity for the camera and lens to function properly
- the data transmission system to connect the remote cameras to the local video monitors that ensure that no undesirable effects are introduced into the video signal
- a synchronization system to ensure that switchings are recording, clean, and free of vertical roll
- video switching equipment to connect multiple video signals from cameras with monitors and video recorders
- a video recording system to produce a record of an event

- video monitors to convert a signal to a visual scene on the face of the output display

- a video controller interface between the alarm sensor system and the alarm assessment system

The video assessment system must be designed as a component of the total intrusion detection system. Interactions between the video system, intrusion sensors, and display system must be considered.

2.4.1.1.4 Alarm Communication and Display

An alarm communication and display system transmits alarm signals from intrusion detection sensors and displays the information to a security operator for action. Although annunciator panels are easy to understand and maintain, they can be expensive, require a large amount of physical space for a large number of zones, and display only a limited amount of information. A state-of-the-art-system uses computer technology and graphics to communicate alarm information to the operator. Characteristics of a good alarm communication system include:

- fast reporting time
- supervision of all data transmission cables
- easy and quick discovery of single-point failures
- isolation and control of sensors
- expansion flexibility

The designer of an alarm display system must decide:

- what information to display
- how to present the information
- how the operator will communicate with the system
- how to arrange the equipment at the operator work station

An alarm communication system is an integrated system of people, procedures, and equipment and must be designed with the special needs and resources of the site in mind.

2.4.1.1.5 Entry/Exit Control

Entry control means allowing entry to authorized personnel and detecting the attempted entry of unauthorized personnel and materials. The measures of effectiveness of entry control are throughput, imposter pass rate (i.e., false accept rate), and false rejection rate. Throughput is defined as the number of authorized personnel allowed access per unit time, assuming that all personnel who attempt entry are authorized for entrance. Imposter pass or false accept rate is the rate at which false identities or credentials are allowed entry. False rejection rate is the rate at which valid identities or credentials are rejected (i.e., entry is prohibited).

Entry control systems consist of the hardware and procedures used to verify entry authorization and to detect contraband (for exit control). Methods of personnel entry authorization include:

- credentials
- personal identification number
- automated personal identity verification

Contraband consists of items such as unauthorized weapons, explosives, incendiaries, and tools. Methods of contraband detection include metal detectors, package searches, and explosives detectors. Special nuclear material detectors are not required at nuclear power plants, but are required at Category I fuel facilities. (The purpose of special nuclear materials detectors used for exit control is to detect the unauthorized removal of nuclear material on persons, in packages, or in vehicles leaving a material access or protected area.) Locks and seals are low technology techniques that have been successfully used for years to deny access to an area or to give indication that access has been gained. An effective entry/exit control system:

- cannot be easily bypassed
- allows observation by the protective force (guards)
- protects guards
- accommodates peak loads
- performs personnel and material control
- blocks passage until personnel and material control are complete
- is under surveillance by the central alarm station
- provides secondary inspections for those who cannot pass the automated inspection
- is designed for both entry and exit

2.4.1.2 Delay

Delay is the second function of a PPS. It is the slowing down of adversary progress. Delay can be accomplished by barriers,[12] locks, and activated delays. The protective force can be considered elements of delay if they are in fixed and well-protected positions. The measure of delay effectiveness is the time required by the adversary (after detection) to bypass each delay element. Although the adversary may be delayed prior to detection, this delay is of no value to the effectiveness of the PPS because it does not provide additional time to respond to the adversary.

2.4.1.3 Response

The response function consists of the actions taken by the protective force to prevent adversary success. Response consists of interruption and neutralization. Interruption is defined as a sufficient number of response force personnel arriving at the appropriate location to stop the adversary's progress. It includes the communication to the protection force of accurate information

[12]In 10 CFR 73.2 a physical barrier is defined as: (1) Fences constructed of No. 11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire or similar material on brackets angled inward or outward between 30 and 45 degrees from the vertical, with an overall height of not less than eight feet, including the barbed topping; (2) Building walls, ceilings and floors constructed of stone, brick, cinder block, concrete, steel or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a building, provided with a barbed topping described in paragraph (1) of this definition of a height of not less than 8 ft; or (3) Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.

about adversary actions and the deployment of the response force. The measure of response effectiveness is the time between receipt of a communication of adversary action and the neutralization of the adversary action.

The effectiveness measures for response communication are the probability of accurate (intelligible) communication and the time required to communicate. The probability of communication having adequate intelligibility and the time required for communication are related as shown in Figure 2-5. The time after information is initially transmitted may vary considerably depending on the method of communication. After the initial period, the probability of valid communication begins to increase rapidly. With each repeat communication, the probability of correct (i.e., adequate intelligibility) and current data being communicated is increased.

Deployment describes the actions of the protective force from the time communication is received until the force is in position to neutralize the adversary. The effectiveness measure of this function is the probability of deployment to the adversary location and the time required to deploy the response force.

Neutralization is the act of stopping the adversary before his goal is accomplished. The effectiveness measure of this function is the response force engagement effectiveness and may be represented by the probability of neutralization (P_N).

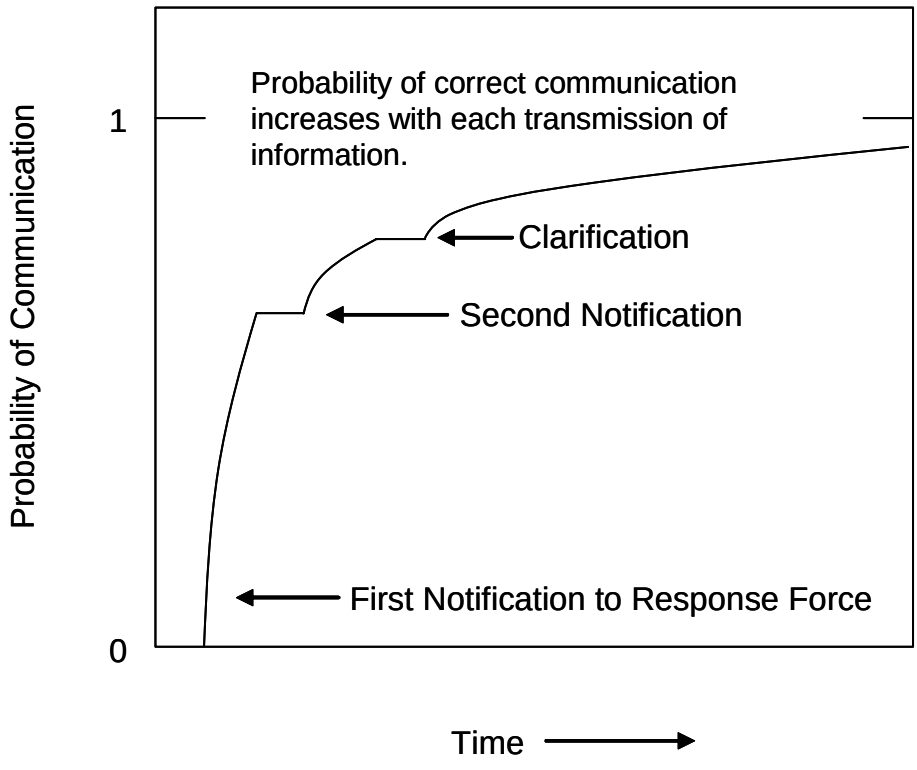

Figure 2-5. Variation of probability of a valid communication with time.

2.4.2 Physical Protection System Characteristics

An effective PPS has several specific characteristics. The effectiveness of the PPS functions of detection, delay, and response and their relationships were discussed previously. In addition, all hardware elements of the system must be installed, maintained, and operated properly to function as intended.

The procedures of the PPS must be compatible with the plant's procedures. Security, safety, and operational objectives must be accomplished at all times. A PPS that has been well engineered will include the following:

- protection-in-depth
- minimum consequence of component failure
- balanced protection

These are discussed in the following subsections.

2.4.2.1 Protection-in-Depth

Protection-in-depth (analogous to the concept of defense-in-depth for safety in which multiple systems must be defeated before safety is compromised) means that to accomplish his goal, an adversary should be required to avoid or defeat a number of protective devices in sequence.[13] For example, an adversary might have to penetrate three separate barriers before gaining entry to a reactor control room. The times to penetrate each of these barriers may not necessarily be equal and the effectiveness of each may be quite different, but each will require a separate and distinct act by the adversary as he moves along his path. The effect produced on the adversary by a system that provides protection-in-depth will be:

- to increase his uncertainty about the system
- to require more extensive preparations prior to attacking the system
- to create additional steps where the adversary may fail or abort his mission

2.4.2.2 Minimum Consequence of Component Failure

It is unlikely that a complex system will ever be developed and operated that does not experience some component failure during its lifetime. Causes of component failure in a PPS are numerous and can range from environmental factors (which may be expected) to adversary actions beyond the scope of the threat used in the system design. Although it is important to know the cause of component failure to restore the system to normal operation, it is more important that contingency plans are provided so the system can continue to operate. Requiring portions of these contingency plans to be carried out automatically (so that redundant equipment automatically takes

[13]In the International Atomic Energy Agency publication *Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage* published in 2007, the term "defence (sic) in depth" is used to describe the concept that defense-in-depth (against sabotage) involves cooperation and planning among those responsible for plant operations, safety, security, emergency preparedness, and other government agencies at all levels to provide protection against sabotage events. Thus, protection-in-depth is analogous to "defence (sic) in depth" in that multiple layers must be defeated before the undesired event occurs.

over the function of disabled equipment) may be highly desirable in some cases. Note that automatic actions may include administrative controls for response force personnel to respond given a specific component failure before the cause of the failure has been identified where specific component failure may be indicative of sabotage. Backup power (secondary power supply) should be designed and implemented to ensure critical security systems continue to function as intended to maintain security system effectiveness. Some component failures may require aid from sources outside of the facility to minimize the impact of the failure.

2.4.2.3 Balanced Protection

Balanced protection implies that no matter how an adversary attempts to accomplish his goal, he will encounter equivalently effective elements of the PPS. Consider, for example, the barrier surface that typically surrounds a reactor control room. This surface may consist of:

- walls, floors, and ceilings of several types
- doors of several types and equipment hatches in floors and ceilings
- heating, ventilating, and air conditioning openings with various types of grills

For a completely balanced system, the minimum time to penetrate, and bullet resistance of, each of these barriers would be equal, and the minimum probability of detecting penetration of each of these barriers would be equal. However, complete balance, with respect to delay, is probably neither possible nor desirable. Certain elements, such as walls, may be extremely resistant to penetration not because of physical protection requirements, but because of structural or safety requirements. Door, hatch, and grille delays may be considerably less than wall delays and still be adequate to meet physical protection system objectives. A balance between overdesigning and underdesigning, being conscious of resource availability, should be achieved. For example, installing a simple hollow-core fire door intended as a barrier in a wall that is two-foot-thick reinforced concrete does not take advantage of the significant delay provided by the wall. Likewise, installing a costly vault door that would take several minutes to penetrate with explosives does not produce balance if the wall composition is such that penetration by hand tools could be accomplished in a few seconds.

Finally, features designed to protect against one form of threat should not be eliminated because they overprotect against another threat. The objective should be to provide adequate protection against all threats on all possible paths and to maintain a balance with other considerations, such as cost, safety, and structural integrity.

2.5 Analyze the Physical Protection System Design

The fourth major activity in the development of a PPS design, as shown in Figure 2-2, is *analyze PPS design*. The PPS design that has been developed to meet the objectives of the protection system (e.g., providing high assurance of protection against significant core damage and sabotage of spent fuel) should be analyzed to determine the effectiveness of the design in meeting those objectives. While this analysis can take one of two forms, quantitative or qualitative, the

preferred approach is a rigorous quantitative analysis.[14] But an acceptable analysis method, applicable to design certification and combined license applicants, is described in Reference 1 (i.e., *Nuclear Power Plant Security Assessment Format and Content Guide*. This analysis method utilizes both quantitative and qualitative elements. The licensed NRC power reactor fleet utilizes this method.

A PPS is a complex configuration of detection, delay, and response elements. Using available tools and techniques, the PPS can be evaluated for its effectiveness.[15] Such techniques identify system deficiencies, evaluate improvements, and perform cost versus system effectiveness comparisons. The approach for analyzing the design of a PPS involves three activities:

- pathway analysis (i.e., identification of potential adversary paths and associated effectiveness measures)
- neutralization analysis (i.e., estimating the effectiveness of the protection and/or response force in preventing the adversary for accomplishing his goal)
- risk assessment (i.e., estimating the overall effectiveness of the PPS as a component of risk)

These activities are briefly discussed in the following subsections.

2.5.1 Pathway Analysis

2.5.1.1 Adversary Paths

Pathway analysis involves identifying and analyzing the paths (through a facility) that an adversary might take during his theft or sabotage attempt (see Section 2.5.1.4 for a discussion on identifying potential paths). An adversary path is an ordered series of actions against a target that, if completed, results in successful theft or sabotage. Figure 2-6 illustrates a single sabotage path of an adversary who wishes to destroy a pump in a high security area. Protection elements along the path will detect and delay the adversary.[16] Figure 2-7 describes example security elements along the path.

2.5.1.2 Effectiveness Measures

The goal of an adversary is to complete a path with the least likelihood of being stopped by the PPS. To achieve this goal, the adversary may attempt to minimize the time required to complete the path. This strategy involves penetrating barriers with little regard to the probability of being detected. If the adversary completes the path before guards can respond to interrupt his activities, he is successful. Alternatively, the adversary may attempt to minimize detection with little

[14]A quantitative analysis can be performed when a PPS is designed to protect assets that, if lost, would result in unacceptably high consequences, even if the probability of an adversary attack is low.
[15]These tools and techniques are applicable in the initial design of a PPS and are also appropriate for reevaluating the design as changes occur in the threat or the physical design of the plant being protected.
[16]Remember, the function of detection includes not only sensor activation but also alarm communication and assessment.

regard to the time required. If the adversary completes the path without being detected, he is successful.

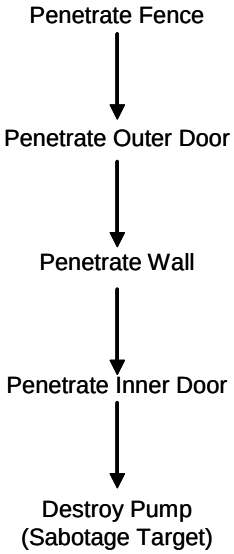

Figure 2-6. Example sabotage path.

Adversary Action	Delay Element	Detection Element
Penetrate Fence	Fence Fabric	Fence Sensor
Penetrate Outer Door	Door Hardness	Sensors on Door
Penetrate Wall	Wall Hardness	Personnel Hear Noise
Penetrate Inner Door	Door Hardness	Sensors on Door
Destroy Pump	Time Required to Sabotage Target	Loss of Pump

Figure 2-7. Protection elements along the sabotage path.

One measure of PPS effectiveness is the comparison of the minimum cumulative time delay along the path (T_{MIN}) compared to the guard response time (T_G). Guard response time includes the total time needed to communicate the assessed alarm to the response force, the time needed by the response force to obtain the appropriate response force tools (e.g., weapons), and the time needed by the response force to travel in adequate numbers to the location where the adversaries can be interrupted.[17] An adequate PPS provides enough delay for the guards to respond. Figure 2-8 illustrates the minimum time measure of effectiveness. For an effective system, T_G must be less than T_{MIN}. System improvements are achieved by decreasing T_G or by adding protection elements with more delay to increase T_{MIN}. The disadvantage of this measure of effectiveness is that no consideration of detection is involved. Delay without prior detection is not meaningful; the response force must be alerted in order to respond and interrupt the adversary. Therefore, the minimum time measure alone is not the best measure of system effectiveness.

Another measure of effectiveness is the cumulative probability of detecting the adversary before his mission is completed. An adequate protection system provides a high probability of detection. Figure 2-9 illustrates the cumulative probability of detection measure of effectiveness. For an effective system, P_{MIN} (minimum cumulative detection along path) must be an acceptable value. The disadvantage is that no consideration of delay is involved. Detection without sufficient subsequent delay is not meaningful; the response force may have insufficient time to interrupt the adversary.

[17]In this context, interrupt means that the adversary's progress is stopped by the response force such that if the adversaries do not stop the activity they are conducting and engage (i.e., fight) the response force, they can be killed.

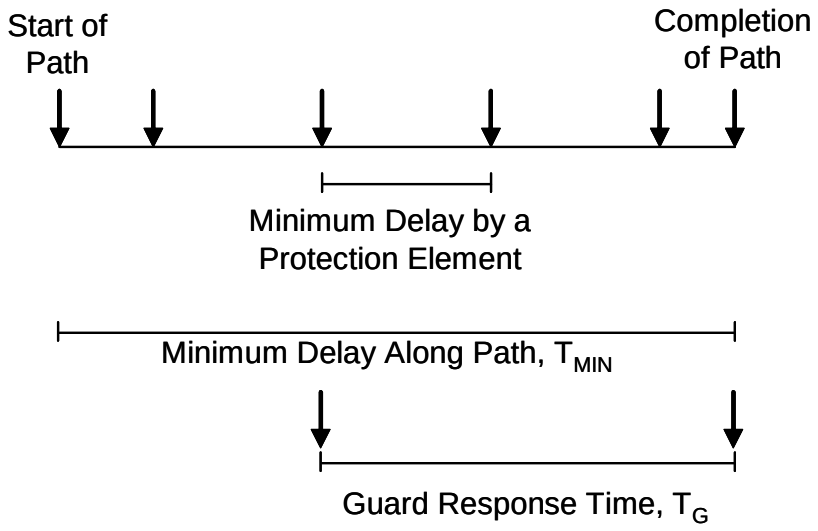

Figure 2-8. Minimum time as a measure of effectiveness.

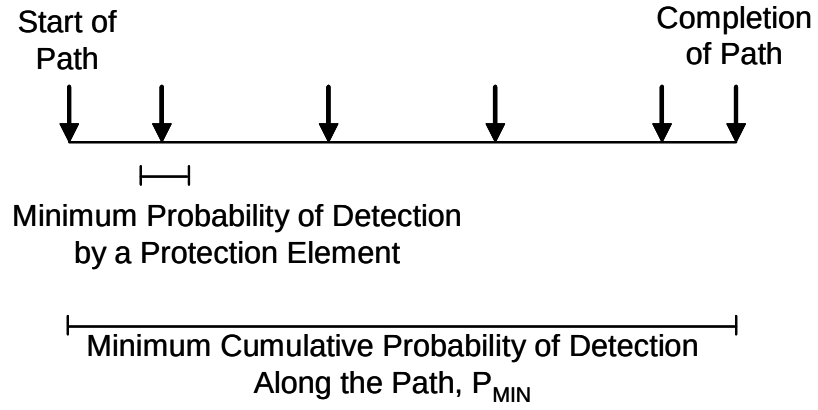

Figure 2-9. Cumulative probability of detection as a measure of effectiveness.

Neither delay time nor cumulative probability of detection alone is the best measure of effectiveness. A better measure of effectiveness is "timely detection." Timely detection is the minimum cumulative probability of detecting the adversary while there is enough time remaining for the response force to interrupt[18] the adversary. Figure 2-10 illustrates the timely detection measure of effectiveness.[19] The delay elements along the path determine the point by which the adversary must be detected. That point is where the minimum delay along the remaining portion of the path (T_R) just exceeds the guard response time (T_G); i.e., the sum of the individual delay times associated with each delay element just exceeds T_G.[20]

[18]See previous footnote.

[19]Here point estimates are used for detection probabilities and times. More sophisticated analyses consider the uncertainty in these variables.

[20]It is recognized that in an actual application one strives to have T_R do more than "just exceed" T_G (to account for all manner of uncertainties). However, for the sake of *defining* the concept of the critical detection point, T_R just needs to "exceed" T_G.

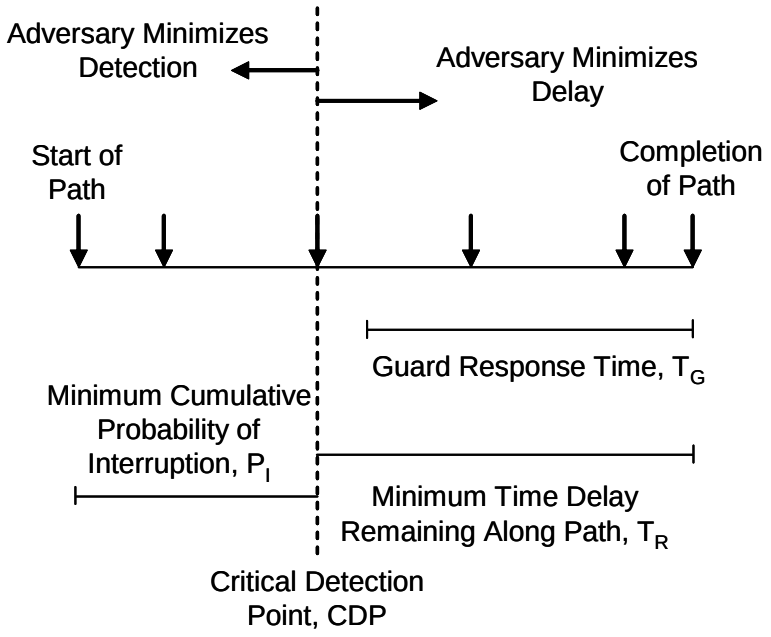

Figure 2-10. Timely detection as a measure of effectiveness.

This point is the critical detection point (CDP). Minimum cumulative probability of interruption (P_I) is the cumulative probability of detection from the start of the path up to the CDP. P_I is used to represent this value to differentiate it from the total cumulative probability of detection because it only considers detection up to the CDP.[21]

2.5.1.3 Critical Path

Typically there are many adversary paths into a facility. The critical path is the path with the lowest probability of interruption.[22] The critical path characterizes the effectiveness of the protection system in detecting, delaying, and interrupting the adversary. Because the critical path in effect defines one component of the overall PPS effectiveness (i.e., P_I), it is important to assure that all potential paths into a facility have been identified. A technique for identifying the paths is presented in the next subsection.

2.5.1.4 Adversary Sequence Diagram

There are three basic steps in creating an adversary sequence diagram (ASD) for a specific site. These include:

- Modeling the facility by separating it into adjacent physical areas
- Defining protection layers and path elements between the adjacent areas
- Showing path segments between the areas through the path elements

[21]To calculate P_I, an assumption is made that the adversary will try to minimize detection before the CDP and minimize delay after the CDP.

[22]The critical path may differ depending on the adversary (i.e., the threat and associated capabilities) and his objective (e.g., theft versus sabotage). Remember, the adversary may involve an insider (one who works at the facility or has access to the facility), and as such, an insider may start at any point along the path.

2.5.1.4.1 Physical Areas

The ASD models a facility by separating it into adjacent physical areas. (See Figure 2-11 for an example.) The ASD represents areas by rectangles. The names of these areas can be changed to model a specific site.

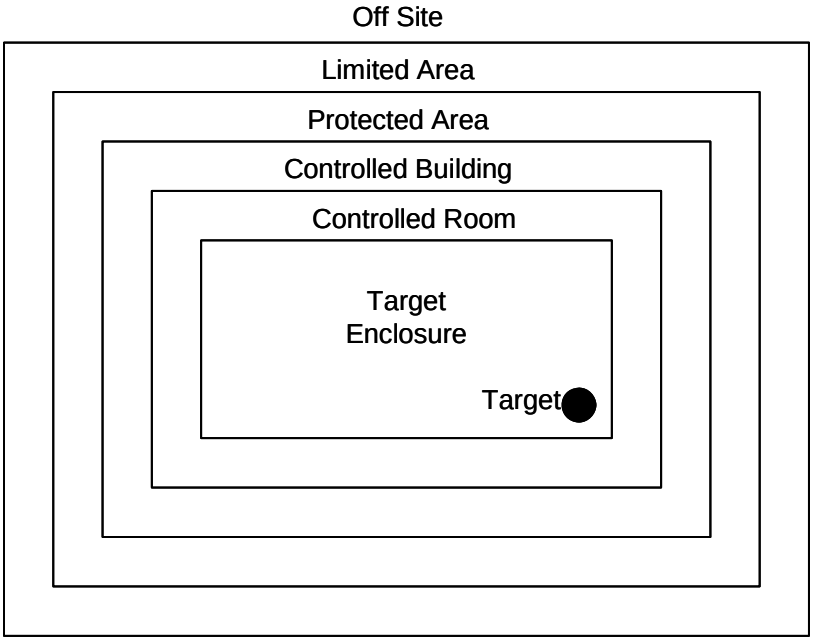

Figure 2-11. Adjacent physical areas—example.

2.5.1.4.2 Protection Layers and Path Elements

The ASD models a PPS by identifying protection layers between adjacent areas (Figure 2-12). Each protection layer consists of a number of path elements (Figure 2-13). Path elements (PEs) are the basic building blocks of a PPS. Examples of the types of PEs and target locations used in an ASD include:

- Path Elements:
  - DUC - Duct
  - EMX - Emergency Exit
  - FEN - Fenceline
  - GAT - Gateway
  - ISO - Isolation Zone
  - DOR - Personnel Doorway
  - PER - Personnel Portal
  - SUR - Surface
  - VEH - Vehicle Portal
  - WND - Window

- Target Locations:
  - FLV - Floor Vault
  - GBX - Glovebox
  - OPN - Open Location
  - TNK - Storage Tank

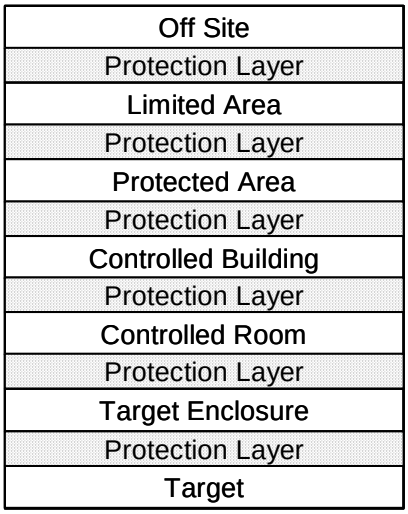

Figure 2-12. Depiction of protection layers between adjacent areas.

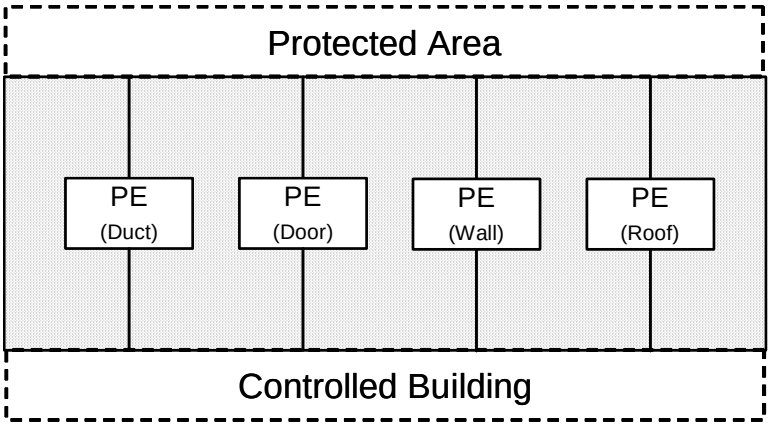

Figure 2-13. Depiction of protection layer consisting of path elements between two areas.

2.5.1.4.3 Path Segments

The ASD represents path segments between areas, through the PEs by lines. Each PE consists of path segments to which delay and detection values are assigned. Both entry and exit parts of a path can be modeled (Figure 2-14). The entry part is from offsite to the target, and the exit is from the target back to offsite. A given PE may be traversed once, either on entry or exit, or it may be traversed twice, on entry and in the opposite direction on exit.

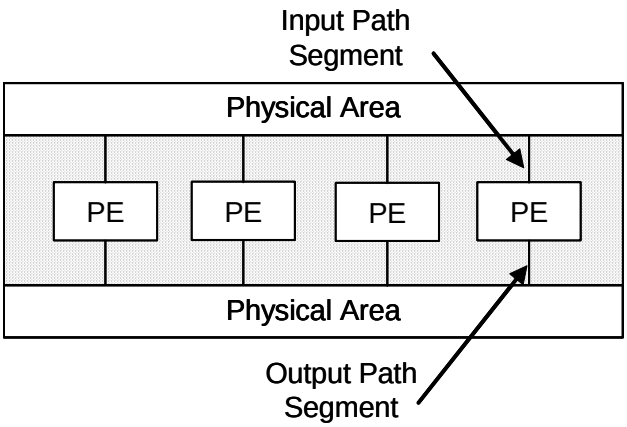

Figure 2-14. Path elements—input and output path segments.

2.5.1.4.4 Basic (Generic) Adversary Sequence Diagram

The basic (or generic) ASD is given in Figure 2-15. The adversary attempts to sequentially defeat an element in each protection layer as he traverses a path through the facility to the target. The ASD represents all of the credible paths that an adversary might take to reach a target.

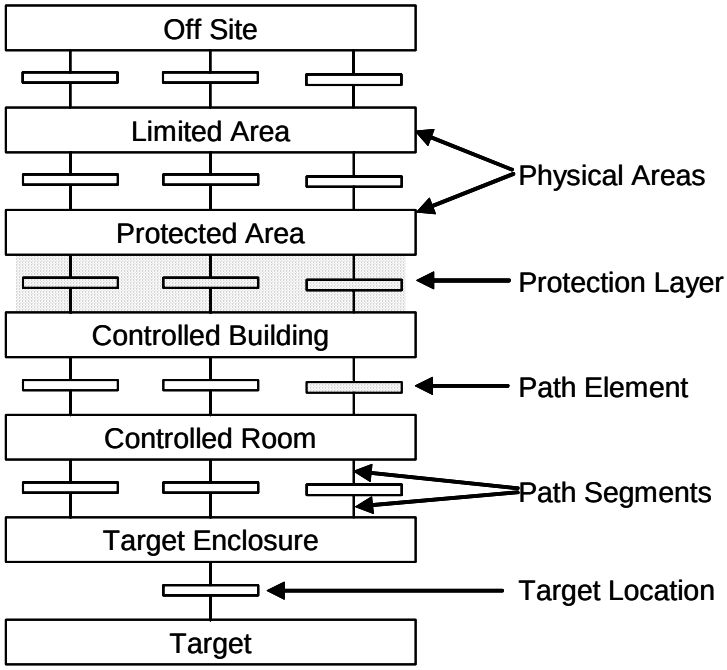

Figure 2-15. Basic adversary sequence diagram.

For a sabotage analysis, only the entry paths would be evaluated, and the path elements would be assumed to be traversed in only one direction. For a theft analysis, the ASD shown would be considered to be traversed twice—on entry to the target and on exit from the target.

Sometimes it will be necessary to deviate from the orderly sequence of physical areas and protection layers of the generic ASD in order to create an accurate site-specific ASD. There are two occasions in ASD development when this is necessary:

- jump
- bypass

A jump is used to model a site element that does not directly connect to the adjacent area shown on the generic ASD. For example, if there were a wall that was common to the controlled building and to the target enclosure, then a jump would exist. A path would exist that would allow the adversary to move from the controlled building directly into the target enclosure (see Figure 2-16).

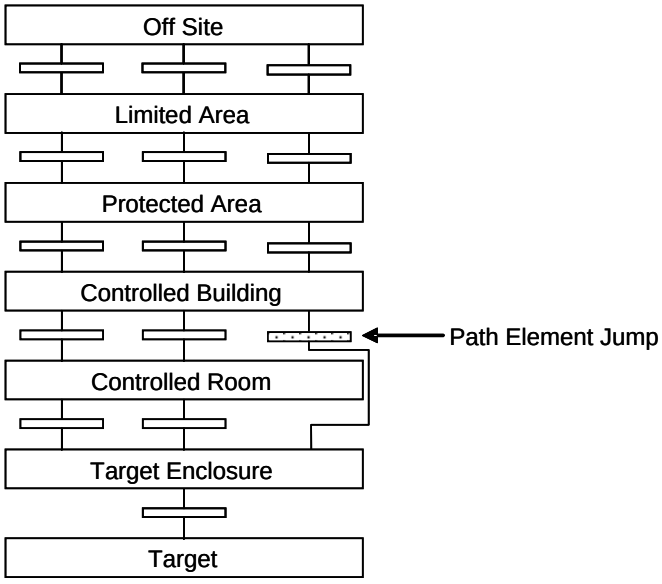

Figure 2-16. Adversary sequence diagram with a jump.

A bypass is used to model the absence of a protection layer. If all the path elements in a layer between two physical areas are removed (or do not exist), then a bypass exists (see Figure 2-17).

The ASD, then, serves as a useful tool to represent all the detection and delay elements in a PPS. By graphically representing all the protection elements by layer, the analyst has a simple picture of adversary paths into a facility and subsequently to the target(s).

2.5.2 Neutralization Analysis

2.5.2.1 Introduction

The majority of the following discussion on neutralization analysis was taken, with some slight modifications, from [Ref. 6].

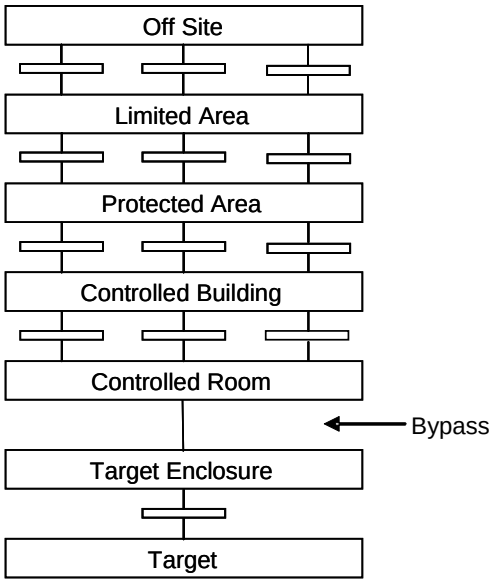

Figure 2-17. Adversary sequence diagram with bypass.

The PPS at a nuclear facility consists of detection, delay, and response functions. The purpose of the response function is to render the adversary incapable of completing his goal. The response function at a facility can be characterized by collecting the appropriate data. However, the analyst must still develop some measure of effectiveness for response. For *response*, the measure of effectiveness is *probability of neutralization (P_N)*.

The determination of this probability requires information about the response forces, the threat, and the PPS, as well as the choice of a methodology for estimating P_N. The following subsections identify the necessary information for determining the probability of neutralization and identify approaches and/or tools for estimating P_N. It should be noted that while approaches and tools exist to estimate P_N, no acceptable standardized methodology exists for calculating P_N.

2.5.2.2 Terminology and Definitions

Before attempting to determine the effectiveness of a response force in neutralizing an adversary force, some terms must be defined. An engagement is defined as an event where two opposing forces, such as the response force and an adversary force, use weapons and tactics in an attempt to achieve their respective goals. Obviously, because many random variables are involved in the engagement, there are many possible outcomes. A win is defined as one of the following outcomes of the engagement: the adversary force is killed, is captured, or abandons the attack and flees.

Probability of neutralization is defined as:

$$P_N = N(\text{wins}) / N(\text{engagements})$$

The number of engagements in the denominator is a statistically significant number in accordance with the Law of Large Numbers. This law states that as the number of times in which an event is repeated becomes larger and larger, the proportion of successful outcomes will tend to come closer and closer to the actual probability of success. In using the defining equation in an analysis process, it should be kept in mind that all engagements must have the same initial conditions and that there are only two possible outcomes per engagement: win or loss.

There are two types of processes that can determine the outcome of an event: deterministic or stochastic.

1. A deterministic process is one in which results or outcomes are causally determined either by preceding events or by natural laws. When an event is governed by deterministic processes, the outcome only needs to be calculated once because, given the same initial conditions, the event will always have the same outcome.

2. Unfortunately, actual engagements are stochastic processes. A stochastic process is one in which various random outcomes are possible because the process involves random variables. The probability of casualty (P_C) attributed to a weapon is an example of a random variable in an engagement. Figure 2-18 illustrates the probability of casualty versus range for a generic handgun (HG) and a generic semi-automatic rifle (SAR).

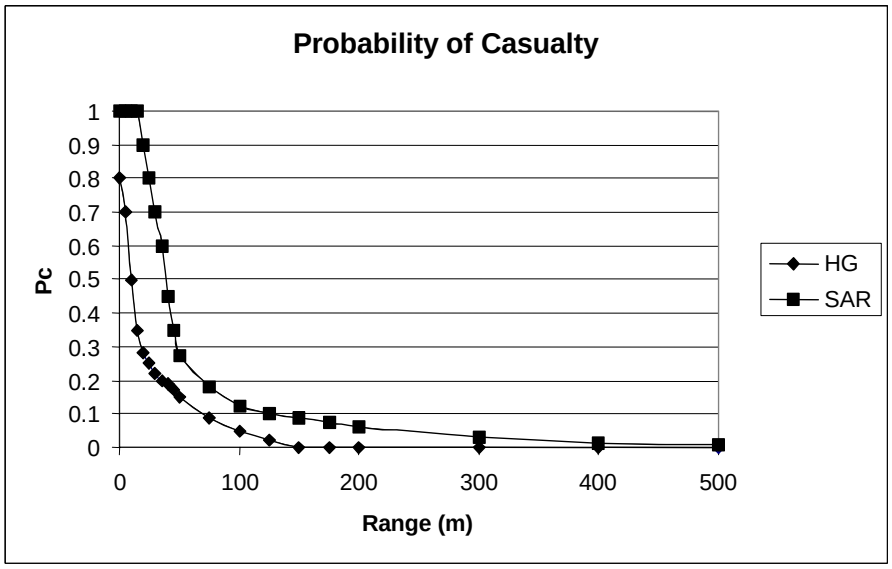

Figure 2-18. Probability of casualty vs. range.

2.5.2.3 Threat Data

Neutralization analysis requires data on the threat, the response, and the PPS. Threat data include threat type and numbers, targets, goals, and other information provided in the DBT. Information about the threat necessary for P_N analysis is summarized in Table 2-1.

Table 2-1. Threat Posture Data

Data Needs	
Target	Special tactics: • ambush • diversion • vehicle bomb
Strategy	
Type	
Number	
Weapons	Body armor
Transport	Communications
Training	Path delay in
Equipment	Target task time
	Path delay out

2.5.2.4 Response Force Data

Similar, but more detailed, information is required about the response forces to determine P_N. In addition to response force posture data, listed in Table 2-2, the rules of engagement and order of battle for each target must be known. The response force posture data contains information about weapons, strategies, numbers of guards, transport, response times, etc., for each target.

Table 2-2. Response Force Posture Data

Data Needs	
Strategy	Body armor
Guard types	Communications
Numbers	Response times: • alarm communication • assessment • deployment order • preparation • travel • deployment
Weapons	
Locations	
Transport	
Tactics	
Training	
Equipment	

Rules of engagement include the conditions and procedures under which various elements of the response force must operate, including when the use of deadly force might be authorized. For the purposes of P_N analysis, it is sound practice to collect sufficient information to construct a table for each target similar to that shown in Table 2-3. As shown in the table, the rules of engagement for each response group or type of responder should include a strategy and an objective, as well as tactics and techniques.

Table 2-3. Rules of Engagement

Response	Strategy	Objective	Tactic	Technique
Target posts				
Other posts				
Patrols				
Tactical teams				
Local Law Enforcement Agencies (LLEAs)				
Other				

Strategies for Table 2-3 could include, but may not be limited to:

- deterrence
- denial
- containment
- pursuit
- recapture/recovery

Each strategy should have an objective, which may include:

- observation
- delay
- interruption
- neutralization
- arrest
- backup

A strategy is implemented through the use of tactics. Tactics are very dependent on the facility, competent authority regulations, and the organization that trains and controls the response. Tactics can include:

- engage at will
- engage on command
- engage on necessity
- coordinated engagement

Finally, there are the techniques that the response force uses with each tactic-strategy combination. Techniques may include, in increasing order of force:

- verbal command
- non-lethal force
- deadly force
- other

The order of battle as defined here is the temporal order in which individual guards or groups of responders are encountered by the adversary. The encounters may occur either as the adversary traverses the path to and from the target or as successive responders arrive at a specific battle site and engage the adversary. The order of battle is target-specific, so it is recommended that a table such as Table 2-4 be completed for each target along the most vulnerable path of each target.

Table 2-4. Example Order of Battle

Target: Vault		Condition: Offshift	
Response	**Type**	**Numbers**	**Time**
1st	Portal guards	2	0 sec
2nd	Interior post	1	30 sec
3rd	Foot patrol	1	60 sec
4th	Special Response Team	5	180 sec
5th	LLEA	4	30 min

2.5.2.5 Neutralization Analysis Methods

Methods for determining P_N can be grouped into the following categories:

- expert judgment (opinion), including tabletop analyses
- simple numerical calculations
- complex numerical simulations (computerized war games)
- physical engagement exercises (force-on-force)
- actual engagements

Each category has its advantages and disadvantages, primarily in terms of time, cost, and accuracy.

Expert judgment is the opinion of one or more subject matter experts about the effectiveness of the response forces. This opinion must be tempered by the background and experience of the expert, knowledge of the response forces at the facility, and knowledge of the threat. Expert judgment is difficult to verify and, unless the same expert is involved in all of the estimations, results can vary from site to site and even target to target. Further, if two or more experts disagree, there is no way to tell if the P_N is valid.

Tabletop (or sand table or military map) analysis involves using a map or site schematic with either icons or figurines to represent combat elements. This method has been used in warfare at least since Roman Legion times. Commanders can place the icons in various positions on the map and debate the outcome of possible engagements. A crucial element for tabletop analysis is the method used to determine the outcome of engagements. Expert judgment, data tables, or a set of rules with simple numerical calculations are the most common methods of determining outcomes of engagements. A sophisticated tabletop analysis method could include both quantitative and qualitative elements such as: timeline analyses, blast analyses, calculations of prob-

ability of detection, and a determination that P_N is adequate by showing an adequate number of response force members, adequately armed and trained, can reach protected positions in a timely manner to neutralize a DBT attack.[23]

Simple numerical calculations are often used in place of or to augment expert judgment determinations. Simple numerical calculations include data tables, curve-fitted equations, continuous time Markov chain (CTMC) methods, and Monte Carlo methods. Figure 2-19 is an example of a data table. The figure presents a comparison of a curve-fit equation with the results of a more complex CTMC solution.

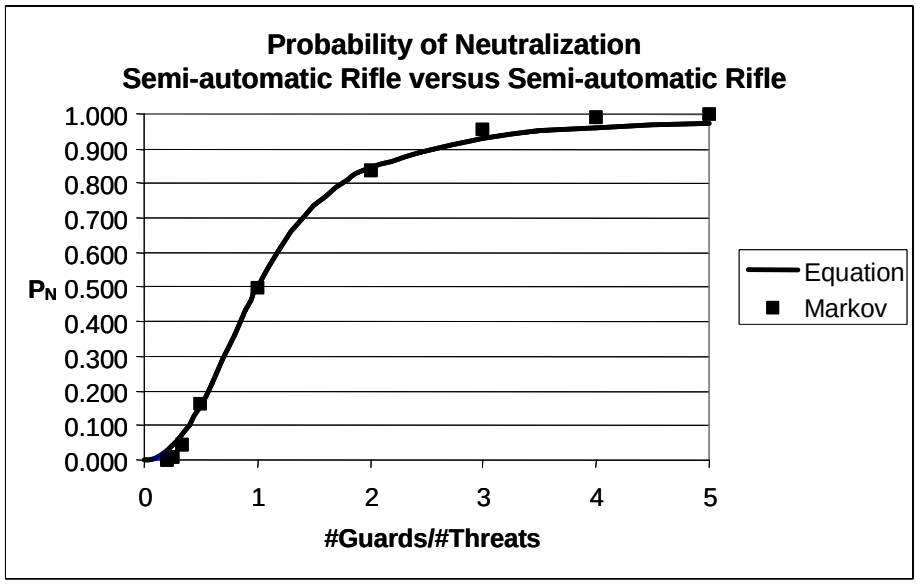

Figure 2-19. Curve-fit equation and Markov chain solution.

Because actual engagements are stochastic processes, the analysis of an engagement must involve a solution technique that incorporates probabilities. Two preferred methods are the Markov Chain method and Monte Carlo simulations.

The Markov Chain method is a path-independent stochastic process in which probabilities of occurrence of future states depend only on the present state or the immediately preceding state. This process is used in [Ref. 7] to develop a state transition diagram and solve the resulting time-dependent transitions from initial state to all probable outcomes of interest. The general development and solution of CTMC is discussed in [Ref. 8]. Figure 2-20 illustrates the state transition diagram, with the transition rates listed as Greek variables between the various states.

[23]This method of conducting tabletop analyses has been used by NRC power reactor licensees to show that the high assurance objective of protection can be met for certain conditions. A baseline inspection program that assesses protective strategy components and a force-on-force exercise program are both also used by the NRC to ensure licensees are maintaining the high assurance objective.

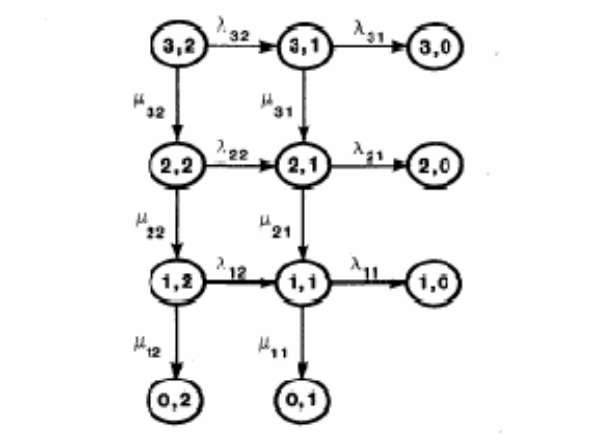

Figure 2-20. Markov chain state transition diagram.

The Analytic System and Software for Evaluating Safeguards and Security pathway analysis computer modeling tool has a Neutralization Module [Ref. 9] and it is an example of a numerical method based on Markov chains. This computer methodology uses probability of kill (P_K) data for various weapons and analysts' descriptions of firing posture, exposure, and other factors to simulate engagements in a manner similar to battles fought in the 1700s; that is, all the combatants stand in a line and fire at each other. A Markov chain is constructed to determine P_N as a function of successive volleys fired by both sides. The main advantages of such simple numerical calculations are (1) low cost and (2) reproducible results, as long as the same input data are used.

Monte Carlo methods involve the use of random sampling techniques. Monte Carlo computer simulations are used to obtain approximate solutions to mathematical or physical problems involving a range of variables, each of which has a calculated probability of being the solution.

Table 2-5 presents an example of a Monte Carlo process for determining the outcome of individual engagements. Two coins are flipped to determine the results of a guard and a threat each firing one shot at the other. A "head" means that the shooter missed his target, and a "tail" means that the target was killed. Thus the implied probability of casualty of each weapon is 50%. One possible outcome, number 1, is that both shooters miss. In this case, the coins are flipped again, representing a second shot. The process is repeated until the engagement outcome obtained is either possibility 2, 3, or 4. If a statistically significant number of engagements are evaluated in this manner, and all wins and losses are recorded, the probability of neutralization for this specific type of engagement can be calculated using the defined formula presented above. It is interesting to note that even though the implied weapon probability of casualty is 50%, the probability of neutralization for this engagement is 66.7%.

Computerized engagement simulations are representative of the third category. The Joint Conflict and Tactical Simulation (JCATS) software tool (developed for the Department of Defense by Lawrence Livermore National Laboratory) [Ref. 10] will be used as an example. In JCATS, modeled adversary entities attack the facility while guard entities try to prevent the adversaries from completing their sabotage or theft scenarios. The first step in running JCATS is the development of a three-dimensional model of the facility. This model includes physical objects (e.g.,

Table 2-5. Monte Carlo Simulation of 1 vs. 1 Engagement								
Outcome	**1**		**2**		**3**		**4**	
Combatant	guard	threat	guard	threat	guard	threat	guard	threat
Toss Result	H	H	T	H	H	T	T	T
Represents	misses	misses	hits	misses	misses	hits	hits	hits
Shot Result	alive	alive	alive	dead	dead	alive	dead	dead
Net Result	Shoot again		win		loss		win	

fences, buildings, and towers), personnel entities (e.g., guard and adversary), and equipment (vehicles, armament, explosives, and tools). All personnel entities are controlled by human operators. The operators that control the guard forces communicate through headsets so that they can coordinate their movements with each other. The adversary force operators also communicate through headsets. An operator can operate a single entity or multiple entities during a simulation. Guards and adversaries interact with each other as they come in view based on line of sight. When an entity uses a weapon to try to kill another entity, the code uses probability of hit/probability of kill (P_H/P_K) tables for the weapon to calculate the odds that a shot at a particular distance would be able to hit another entity. Simulations end when either the adversaries have completed their tasks or the guards have been able to neutralize the adversaries.

Simulated physical engagements are known as force-on-force (FOF) exercises. Force-on-force exercises are not actually evaluation methodologies but rather should be considered training exercises or validation exercises. At a real facility, FOF requires four groups: mock adversaries, mock responders, referees (controllers), and the on-duty response force personnel. These exercises are expensive in terms of both personnel and planning, are usually run only a few times at a facility, and can produce skewed results.[24] Statistically, there are usually not enough engagements to produce a probability of system win with a high confidence level.

Actual engagements have one big advantage: the outcome is a known fact. Obviously, comparison of actual engagements results with either live fire or simulation exercises can be complex and costly; however, such comparisons prove the validity of simulation techniques.

2.5.3 Risk Analysis

The underlying premise of this chapter is that the design and evaluation of a PPS must be done from a system standpoint. In this way, all components of detection, delay, and response can be properly weighted according to their contributions to the PPS as a whole. At a high level (i.e., the decision-maker or site management level), the effectiveness of a PPS (and thus the design requirements necessary to achieve that effectiveness) must be balanced against available resources. Without a methodical, defined, analytical assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility.

[24]However, it should be recognized that drills exercising several elements of a PPS and limited scope performance tests exercising one element of a PPS are less costly and provide valuable methods for measuring PPS effectiveness.

In evaluating the effectiveness of a PPS, the risk associated with the facility from malevolent activities is given by:

$$R = F_A * [1 - (P_I * P_N)] * C$$

where:

R = Risk to society of an adversary gaining access to, or stealing, nuclear material.

F_A = Frequency of adversary attack. It is very difficult to determine what this value should be. Clearly, simple use of past history to estimate this value may not be appropriate given current understanding of today's threat environment.

P_I = Probability of interruption. The probability that the defined adversary will be interrupted by the response force in time to stop the adversary from accomplishing his objectives.

P_N = Probability of neutralization. For a given adversary and response force given interruption has occurred, the probability that the response force will defeat the adversary in an engagement (i.e., prevent the adversary from accomplishing his objective).

C = Consequence associated with the loss of the targets the PPS is designed to protect. For a nuclear power plant, the consequence is typically associated with a radiological release. Other consequence measures may be used. The appropriate consequence measure to be used in the PPS risk calculation is established by the NRC.

Typically during the design of PPS, the assumption is made that an attack occurs. Thus the risk equation becomes:

$$CR = [1 - (P_I * P_N)] * C$$

where:

CR = Conditional risk (i.e., the risk given an attack).

The term $P_I * P_N$ is typically referred to as the probability of system effectiveness (P_E) and represents the probability that the PPS prevents the consequence given an attack.

The focus of the PPS design process is on maximizing P_E.

2.6 Is Design Acceptable?

At this point in the PPS design and evaluation process, the risk associated with a particular design is known. The question that must be answered is whether the level of risk associated with the design is acceptable. This requires that the risk be compared against a decision metric. If the risk is less than the decision metric, then the design is acceptable and no further work is necessary. If the risk associated with the design is not less than the decision metric, then the PPS

should be reexamined to determine those areas that, if strengthened (i.e., enhanced), would allow the risk associated with the revised PPS to be acceptable.[25]

The decision metic for NRC-licensed nuclear power plants is "Does the risk associated with the PPS meet the high assurance objective of protection?"

[25]Since the PPS design and analysis process presented in this report is expected to be used in the design of physical security at a new plant, the designer should already be aware of the risk decision metric and should continue iterating on the PPS design until the risk is acceptable.

3. ANALYTICAL TOOLS

There are a number of analytical tools available to the designer/analyst that can be used to evaluate the proposed physical protection system (PPS) for a facility design. Each of these tools has its strengths and weaknesses and is intended to provide the user with different information. These tools may be used independently or in combination to evaluate PPS effectiveness. The manner in which these tools are used will depend on what measure is used to determine PPS effectiveness.

Two major categories of tools exist. The first deals with pathway analysis and the second deals with neutralization. The intent of the following sections is to provide a summary description of some of the major tools available to an analyst. One should not consider the list of tools exhaustive.

3.1 Tools That May Be Used in Pathway Analysis

As discussed in Section 2.5.1, pathway analysis involves identifying and analyzing the paths (through a facility) that an adversary might take during his theft or sabotage attempt. Given the complex nature of commercial nuclear power plants, it is expected that a computerized pathway analysis tool would be most useful in identifying the most vulnerable paths (i.e., the paths most likely to lead to adversary success). The next five subsections identify tools that may be used to identify and/or analyze adversary paths. The final subsection identifies a tool that helps an analyst estimate delay times not included in an access delay database.

3.1.1 Analytic System and Software for Evaluating Safeguards and Security

The Analytic System and Software for Evaluating Safeguards and Security (ASSESS) software is an integrated software package for identifying adversary pathways and evaluating system effectiveness against theft or sabotage of special nuclear material by a spectrum of adversaries: outsiders, insiders, and an insider colluding with outsiders. The probability of detection for each nonviolent insider adversary type is calculated using a reference database of adversary attributes, defeat methods, strategies, and detection performance. Probability of interruption (for theft or sabotage) is calculated for an outsider threat spectrum of terrorists, criminals, psychotics, and extremists. (Note: ASSESS can be used to estimate the probability of neutralization of violent adversaries using the small force engagement attrition model included in the code thus allowing one to calculate a probability of system win for theft or sabotage. In addition, a probability of system win can be calculated for uncorrelated handoff of theft material by various insiders in collusion with outsiders.)

To enquire about a copy of the software, contact the Office of Technology, U.S. Department of Energy (DOE).

3.1.2 Adversary Time-Line Analysis System

The Adversary Time-Line Analysis System (ATLAS) is a software program used to compute the most vulnerable paths for attacks by both an outsider adversary and a violent insider. The most vulnerable paths are computed in two different ways. The first minimizes probability of inter-

ruption (P_I). This is called the critical detection point (CDP) approach, because it is based on locating the CDP. The second minimizes delay after the practical detection point (PDP). These two analyses are complementary analysis approaches.[26]

Another analysis feature identifies elements that are critical to the overall protection system effectiveness. Critical elements are defined as protection elements that, if individually degraded to a critical performance level on entry, will reduce significantly the probability of system effectiveness (P_E).

To enquire about a copy of the software, contact the Office of Technology, U.S. DOE.

3.1.3 Systematic Analysis of Vulnerability to Intrusion

The Systematic Analysis of Vulnerability to Intrusion (SAVI) program is Windows-based software that can be used to determine the optimal path for the adversary to take to attack the facility. It is composed of two main modules; the Facility module and the Outsider module.

The SAVI Facility module is used to construct an ASD as described in Section 2.5.1.4. The SAVI Facility module contains an array of generic protection element types like fences, windows, gates, doors, and walls that can be configured to model appropriate detection, delay, and response safeguards. A database of delay times as well as detection values that are based on performance testing against adversaries with various attributes is provided in SAVI. These default values may be used or, if the user has specific data, allows the user to modify the detection or delay values. Once an ASD is finished, the file is saved and the SAVI Facility module is closed.

The SAVI Outsider module is then used to analyze the facility. The user specifies the threat type (how the adversary is armed and what tools he carries), the response strategy (denial or containment), the attack method (force/stealth or deceit), and the state of the system (dayshift or off shift operations). SAVI then calculates the detection and delay values for each protection element by analyzing all attack methods for the threat and selects the minimum detection and delay values for each element. For a given response force time, SAVI will calculate the facility's most vulnerable path. The algorithm first determines the CDP (for each path) and then calculates P_I. The SAVI software was developed for the Department of Energy by Sandia National Laboratories and Apogen Technology (formerly SEA, Inc.) [Ref. 11].

To enquire about a copy of the software, contact the Office of Technology, U.S. DOE.

3.1.4 Estimate of Adversary Sequence Interruption

The Estimate of Adversary Sequence Interruption (EASI) tool is an Excel spreadsheet that can be used to calculate P_I for a single path [Ref. 2]. The user constructs a sequence of tasks along an adversary path that takes the adversary from offsite to completing the act of sabotage or theft. The data that the code needs is the mean and standard deviation of the delay time needed to accomplish each task, the probability of detection for any alarm that may be triggered along the path by the adversary, the probability of (guard) communication, and the mean and standard de-

[26] The primary approach is the CDP approach. The PDP approach may identify paths that the CDP approach may not. A PDP analysis should *never* be performed without also performing comparable CDP analyses.

viation of the response force time. Once all the data have been entered, the code calculates P_I for the path.

The EASI software can be downloaded from the web at http://books.elsevier.com/companions/0750673672/.

3.1.5 Vulnerability of Integrated Security Analysis

The Vulnerability of Integrated Security Analysis (VISA) methodology [Ref. 12] is a tabletop analysis technique that utilizes the expert judgment of the members of the vulnerability analysis team and any performance data (e.g., probability of detection for a specific sensor) that are available to the team to analyze the effectiveness of a PPS. The process is step-dependent, meaning that developed scenarios, including the identified paths the adversaries take, are broken down into individual steps, evaluated as to the probabilities of detection, assessment, interruption, and neutralization (as assigned by the team), and then scored. The VISA methodology can be used on its own for a quick analysis of a facility or it can be used in conjunction with other tools (e.g., ASSESS). As with any tabletop analysis technique, care should be taken to ensure that the analysis is comprehensive (i.e., analysis of all threats to and paths into a facility have been examined) if a total PPS effectiveness analysis is being performed.

Copies may be obtained from the NRC staff.

3.1.6 Access Delay Knowledge-Based System

The Access Delay Knowledge-Based System (ADKBS) is a software analysis tool that was developed to assist in estimating penetration delay times for single or multiple barriers. The ADKBS software was prepared to supplement the database used by the ATLAS program and other currently applied access delay technologies. The primary purpose of ADKBS is to develop penetration delay time estimates for single or multiple barriers and/or attack methods not specifically addressed by the database alone. It generates these estimates by taking into account existing barrier delay information, rate data, and the installation circumstances of the barrier. The ADKBS software is designed to provide a central source of penetration times and supporting information for barriers for protection system effectiveness evaluations. The ADKBS software is also intended to assist the user in identifying options for upgrading existing access delay elements and to define advanced concepts for new or replacement elements with improved penetration times.

To enquire about a copy of the software, contact the Office of Technology, U.S. DOE.

3.2 Tools That May Be Used to Estimate Probability of Neutralization

The following subsections provide a brief discussion on a select set of neutralization tools. These tools can be used to produce estimates of P_N or may be used to provide input to other tools; however the reader should be aware that there is no acceptable standard as to how P_N should be estimated (calculated).

3.2.1 Joint Conflict and Tactical Simulation

The Joint Conflict and Tactical Simulation (JCATS) software is a tool used to evaluate the effectiveness of a protective force to defend against a predetermined adversary attack objective. Because JCATS is a resource-intensive, man-in-the-loop simulation, the scenario(s) evaluated with JCATS should be considered worst-case as determined by other less costly analyses. When combined with subject matter experts and tabletop evaluations, JCATS provides an effective means for estimating engagement outcomes and validating security system effectiveness.

JCATS was developed for the Department of Defense by Lawrence Livermore National Laboratory to provide a realistic, stress-filled, simulated urban combat training environment and has been adapted by the DOE to model its facilities and specific adversary capabilities.

JCATS simulates the entire combat environment (buildings, vehicles, barriers, combatants, weapons, explosives, etc.) and uses multiple players to control assigned combat systems and resources during the simulation exercise. These combat systems include teams of combatants called units and ground/air mobile platforms armed with direct and indirect fire weapons. The key functional areas modeled in the simulation are:

- movement and individually controlled combat in and around detailed buildings
- movement in and around buildings
- clearing, occupying, and reinforcing buildings
- movement of vehicles and units, to include mounting and dismounting vehicles
- target acquisition using a variety of sensing techniques
- direct fire engagements between combat units
- fratricide
- some human factors (e.g., fatigue, suppression) that affect performance
- environmental factors (e.g., weather, terrain) that affect movement and line-of-sight acquisition
- indirect fire
- barriers

JCATS simulations require data for these key functional areas.

An important aspect of JCATS is that the outcomes of individual engagement events are based on hit and kill probabilities in the form of P_h/P_k tables. Each engagement event outcome is determined stochastically by extracting the event probability from the P_h/P_k table based on event time battlefield conditions and then drawing a random number against that event occurrence probability to establish event success or failure. These individual stochastic results affect the battlefield condition for the next time-step and in turn determine the overall win/loss outcome of the simulated engagement. This randomness reflects the battlefield environment and highlights the importance of synchronization and timing on the overall outcome of the battle.

For the purpose of estimating P_N for worst-case scenarios, each engagement is run in JCATS several times to accumulate overall battle win/loss samples. When combined with appropriate subject matter experts (e.g., those knowledgeable of JCATS's strengths and weaknesses) and more detailed results regarding the severity of the engagement win/loss, results from the JCATS

exercises (i.e., scenarios) can be used to estimate the effectiveness of the physical protection force in neutralizing the adversary force (i.e., P_N).

3.2.2 Tabletop Assessment Methodology

There are several tabletop methodologies and procedural tools for evaluating protection system effectiveness (or estimating potential for neutralization) against specified threats. There are different variations of these methodologies but for the most part these methodologies are applied in a logical, sequenced manner that considers the adversary threat, target attractiveness, malevolent adversary acts, and the potential consequences of adversary success. This assessment also evaluates the existing security system and its ability to protect assets, which include personnel, facilities, equipment, and procedures. A major activity also includes determining a security force's capability to effectively respond, interrupt, and neutralize an adversary attack, which is determined by subject matter experts who develop and analyze various scenarios. Timeline analysis using pathway analysis tools supplemented by blast analyses, delay times of barriers, and calculations of detection probability (i.e., $P_{D)}$ can be used to enhance tabletop methodologies.

3.2.3 Force-on-Force Exercises

Force-on-force (FOF) exercises (i.e., simulated physical engagements) are not actually P_N evaluation methodologies—they should be considered training exercises or validation exercises. However, if well-designed and conducted, they may provide insights about the protective force that may be used by other tools/techniques for estimating P_N. One major reason why FOF exercises should not be used to directly estimate P_N is that these exercises are usually run only a few times at a facility (they are expensive in terms of both personnel and planning); thus, there are usually not enough engagements to produce a probability of system win (i.e., neutralization) with a high confidence level.

4. PHYSICAL PROTECTION SYSTEM DESIGN: BEST PRACTICES

4.1 Risk Assessment

As stated in Chapter 2, conditional risk assessments are conducted to determine the overall effectiveness of a physical protection system (PPS). There are a number of risk assessment methods available to analysts to determine system effectiveness and subsequent risk. The most thorough of these accomplish the following:

- identify PPS objectives
- establish facility design
- design the PPS
- analyze the PPS design (using an integrated systems analysis approach)

Depending on the assessment method used, a risk assessment may be conducted:

- against an existing facility
- against a facility master plan that has been designed but not constructed
- in parallel during the design process

Where possible, it is always best to determine the PPS objectives and incorporate these objectives into the PPS design ***during*** the facility master design process. This is the most cost-effective and efficient method of conducting risk assessments because it mitigates the need for costly redesign and facility upgrades necessary to protect against a design basis threat (DBT). It also provides an opportunity to engineer a PPS design against current and future postulated threats. In addition, it provides opportunities to reduce the cost of the PPS over the life of a facility by reducing reliance on operational programs. For example, if a site could reduce by 10 the number of security force personnel required to meet the high assurance objective by implementing engineered security features, this would result in a cost reduction of (10 people/shift) * (3 shifts/people) * ($175K/year)*(40 years) = $210M minus the cost of the design, implementation, and maintenance of the engineered security features utilized.

For nuclear power reactors in the design stage it is strongly recommended to perform an iterative design and evaluation process as described in the *Nuclear Power Plant Security Assessment Format and Content Guide* [Ref. 1] considering the best practices identified in this chapter and the security system technologies in Chapter 5. It is also recommended to use this document as a technical manual. The result of this iterative design process could yield a more effective, integrated, and cost effective site security strategy. Designs that have not yet completed their vital area designs have the best opportunity to benefit from the performance of such a security assessment.

4.2 Target Identification

Target identification provides the foundation for designing an effective PPS because it determines *what to protect*, while the PPS design determines *how to protect*. Target identification

should not take into account the threat[27] or the difficulty of providing physical protection. In general, target identification should know what the undesirable consequences are, use a robust method to identify the targets, and then identify the targets (or target areas). Targets may include areas within the site, specific equipment, nuclear materials, infrastructure, processes, or other assets that if subjected to a particular threat could have undesirable or unacceptable consequences. For any new commercial nuclear power plant, the set of targets that determine what to protect should be such that if protected, undesired consequences cannot happen (or at least cannot happen because of the malevolent intent of the adversaries).[28]

4.3 Threat Definition

A threat analysis must be completed to determine the threats to a facility. These threats must be determined before an effective PPS can be designed and the PPS must be designed to protect against the defined threat. A threat analysis should result in a formal, detailed description of the threat by a malevolent adversary. The threat definition must describe the physical capabilities, motivations, and potential actions of the adversary. This description should also include both outsider and insider adversary types and capabilities, as well as the potential threat of outsiders working in collusion with insiders. It is necessary for the regulatory agency to ensure that an adequate threat analysis has been completed and that the subsequent DBT is provided to the PPS designers so that they can design an effective PPS.[29]

4.4 Planning and Design

Effective PPS design begins with the planning process. While this is an obvious first step, it is critical to include all necessary stakeholders in the master planning process to achieve a design that meets the requirements of operations, safety, and security. This approach to master planning provides an integrated strategy for engineered design, construction, and maintenance of nuclear power plant facilities that in the long-term is cost-effective and more efficient and helps to reduce short-term decision-making that tends to occur at the project level. Limiting or excluding security representation during the design process will ultimately have a negative impact on PPS effectiveness and invite unnecessary future costs through retrofitting to mitigate an ever-changing threat spectrum. Addressing security concerns that are based on threat-specific assessments of nuclear power plants with engineered PPS design solutions throughout the master planning and design process will ensure adequate and efficient protection of personnel, equipment, property, and infrastructure.

Incorporating effective PPS engineered design elements into the master plan requires subject matter experts representing the detection, delay, and response disciplines. It is also essential to include expert vulnerability analysts who are qualified to assess the identified threats against the

[27]What to protect is determined by the consequences that are to be avoided (e.g., a radioactive release beyond a specified quantity); thus, the *threat* plays no role in determining the targets. However, the *threat* will play a role in determining the degree of sophistication of the PPS.

[28]Targets not susceptible to a given threat (i.e., the given threat does not have the knowledge, skills, tool set, and motivation necessary to attack the targets) are not a target for any scenario that involves that threat.

[29]The Nuclear Regulatory Commission is responsible for identifying the DBT and providing it to the organizations responsible for designing new commercial reactor facilities so that the designers can develop an appropriate PPS for the facility.

identified targets, the performance of a PPS design against the identified threats, and are qualified to determine protection system effectiveness and the associated overall risk.

Best Practices for Planning and Design:

- Establish a security team to provide PPS design requirements.
- Define security team roles, responsibilities, and authority as it integrates with the facility design team.
- Determine the resources necessary to support security design and analysis.
- Identify and document security design requirements early in the facility design process.
- Security design requirements should be based on a threat-specific assessment of nuclear power plants.
- Plan for an iterative process of design, analysis, and redesign and reanalysis.

4.5 Site Selection and Layout Design

4.5.1 Site Selection

Site selection for nuclear power plants will be controlled by competing priorities, demands, and considerations that will significantly influence where the facilities are constructed. These factors, such as operational needs, political constraints, environmental concerns, property availability, cost, and local, state, and federal regulations will present challenges that the planners will have to adequately address during site selection. Therefore it is essential that security concerns be identified and PPS requirements documented early in the site selection process. By addressing security concerns with the proposed site, early in the process, it helps to ensure that the site location is compatible with an effective PPS design. It is also more cost-effective and efficient to resolve concerns during the planning process than attempting to address them after site selection.

4.5.2 Layout Design

The layout design of a site will generally be driven by nuclear power plant operational and functional requirements, safety concerns, and the particular site selected. However, the layout design should also include elements of physical protection that include a layered approach to security (access controls, entry control points, access roads, delivery locations, parking lots, etc.), security area locations (owner controlled, vital, and protected areas), entrances for external response and emergency services, and security force facilities. As part of the site layout design a terrain analysis should be conducted to define terrain characteristics relative to both security and adversary forces. Terrain characteristics should be evaluated to determine:

- Natural and manmade features that may provide vantage points or obstacles.
- Observation points, fields of fire, clear zones, and cover and concealment areas.

- Likely avenues of adversary approach and required security response approaches.
- The traversal time on foot and by vehicle for adversaries and security response.
- Low-lying areas that facilitate use of chemical weapons and obscurants.
- Perimeter requirements for standoff distance, barriers, entry/exit control points, perimeter lighting, etc.

Best Practices for Site Selection and Layout Design:

- Identify and document any security concerns associated with the site under review for selection and the prospective site layout design.
- Ensure to the extent possible that the site location and layout are compatible with an effective PPS design.
- Interior design should consider choke points en route to vital areas/equipment.
- Conduct a terrain analysis as part of the site selection and layout design to define terrain characteristics that may be of tactical importance to the security or adversary force.
- Aircraft approaches should be analyzed with regard to their feasibility of being used to strike areas of concern.

4.6 Designing the Physical Protection System

The purpose of a PPS is to prevent an adversary from completing a malevolent act that subsequently results in unacceptable consequences. The primary functions of a PPS are detection, delay, and response. These functions must be balanced and work effectively together to form an effective protection system. For the system to be effective, the adversary must be detected and sufficiently delayed along his attack path until security forces can respond and neutralize the adversary. The following sections discuss detection, delay, and response. In addition, sections on insider mitigation, additional PPS considerations, and planning for future threat and adversary capability changes are included.

4.6.1 Detection

Detection is the discovery of an adversary action and includes sensing of covert or overt actions. Detection may be performed by a person, such as security force personnel who are assigned to fixed posts or on patrol. However, while security force personnel perform a vital role in the overall protection system and may detect an intrusion, this method of detection is not always the most reliable. Consequently, the probability of detection assigned to this method is generally low. The most effective detection systems are electronic systems and include:

- exterior intrusion sensors
- interior intrusion sensors

- video alarm assessment
- alarm communication and display (AC&D) systems
- entry control systems

For detection to occur:

1. A sensor reacts to a stimulus and initiates an alarm

2. The information from the sensor and assessment subsystems is reported and displayed

3. A person assesses this information and judges the alarm to be valid or invalid

A critical element of detection is the process of assessment, which is determining whether an alarm is valid or invalid and what specific threat, if any, is present. Without this important determination, the cause of the alarm is unknown and the appropriate response may not be provided; thus *detection without assessment is not detection*. As a result, protection system effectiveness may be seriously degraded.

The engineered design and layout of detection systems is a complicated and rigorous process that requires subject matter experts in electrical power systems, fiber optic systems, communications, sensors, video assessment, AC&D systems, delay, and response. In general, however, an effective detection system provides defense-in-depth with site, facility, and target detection systems.

Best Practices for Detection:

- A properly designed detection system incorporates detection at the perimeter through the use of a Perimeter Intrusion Detection and Assessment System, video assessment system capabilities along probable adversary attack paths, and facility and target detection and assessment equipment. In addition, use of extended detection capabilities (i.e., detection that senses outward into the owner controlled area from the protected area perimeter) should be considered.

- An effective external (i.e., perimeter) detection system will include a properly installed Intrusion Detection System (IDS) designed with multiple complimentary sensors, overlapping detection zones, electronic assessment equipment, and reporting capability.

- Measures of effectiveness for detection functions should be the probability of sensing an adversary action and the time required for reporting and assessing the alarm.

- A good detection system is designed using components that have validated performance measures established for operation and the false and nuisance alarm rates are as low as possible for local environmental conditions. In addition, a good detection system has administrative measures implemented to keep nuisance alarms acceptably low (e.g., good housekeeping activities that keep weeds and bushes trimmed near fence lines and animal barriers thus minimizing the potential for interaction with sensors).

- An effective detection system includes an effective assessment system that provides information about the type of alarm received (adversary attack, false, or nuisance alarm).

- Security lighting is an integrated element of the IDS and is essential to enable security forces to maintain continuity of operations during low-light and nighttime hours. A properly designed and installed perimeter security lighting system assists detection and assessment and increases the effectiveness of electronic security systems by sufficiently illuminating the perimeter during low-light conditions and darkness to ensure a high probability of detection, sensing, and assessment.

- A robust detection system includes effective entry and exit controls that not only maximize authorized personnel and vehicle traffic flow but also does so safely and securely. Entry and exit control functions are conducted at access control points (ACPs) and are intended to control the access (entry and exit) of personnel, visitors, and vehicles.

  – ACP functions should include access control, personnel and vehicle searches, and emergency response entry (fire, medical, etc.).

  – The ACP should also provide hardened, secure locations for security forces to defend themselves and their battle space.

  – The priority of an entry and exit control system is to maintain perimeter security.

- Detection system support infrastructure (electrical power, communications, fiber optics, cabling, etc.) should be separate, protected, and dedicated to security systems.

- Unattended openings[30] that intersect a security boundary should be identified.[31] Where possible, electronic detection of unauthorized entry (or exit) should be installed. If electronic detection is neither possible nor practical, then delay barriers should be installed and observation by security personnel should occur with a frequency that allows timely response upon detecting evidence of ingress, egress, or tampering.

4.6.2 Delay

Delay is a major function of a PPS. The PPS should be designed to impede adversary penetration into or exit from a security area or target location and at the target set itself. Delay can be accomplished by passive delay systems such as physical barriers, activated systems such as activated dispensable materials, activated lethal or non-lethal systems, or by the response of security forces. The delay time to penetrate a delay element depends on the type[32] of attack, location of

[30]To deny unauthorized personnel access, openings greater than or equal to 96 in.^{2} and larger than 6 in. in the smallest dimension should be identified. If theft is a concern or if the passing of items that may be used to aid in sabotage or theft must be considered, then the size of the openings is determined by the minimum size of the object or material that will be passed. For additional information see Regulatory Information Summary 2005-04, "Guidance on the Protection of Unattended Openings that Intersect a Security Boundary or Area," dated April 14, 2005.

[31]During the design of a site and its associated buildings and facilities, a concerted effort should be made to identify any unattended openings meeting the specified requirements. Identifying the openings during the design process should allow for a more orderly inclusion of the openings when designing (and subsequently installing) the detection sensors, thereby saving money in the long run.

[32]One type of attack could be by unskilled adversaries who do not have the knowledge or skills to defeat delay elements; thus it could take them a long time to defeat the delay elements. Another type of attack could be by skilled

the attack, the tools and equipment used, and the skill set of the adversary. The task time to breach a delay element is considered delay only if it occurs after detection and assessment of an adversary action.

Effective delay has become increasingly important in the design of a PPS to counter the increase in adversary capabilities. The application of robust delay systems not only includes improved fixed barrier designs, but also includes activated dispensable materials and activated lethal and non-lethal systems. These enhanced delay systems are important because they allow trade-offs with the numbers of on-site security forces, providing a cost-effective alternative to increasing the numbers of additional security force personnel to meet new threats and adversary capabilities.

Physical barriers are a vital element of the overall security system, serving a dual purpose. Properly designed and installed barriers are used to control the authorized entry and exit of personnel and vehicles by channeling the flow of personnel and vehicles through designated control points where access authorization can be verified and inspections and searches conducted. An equally important purpose for barriers is to physically impede unauthorized entry and exit.

Physical barriers are obstructions designed or deployed to impede, disrupt, turn, or block the movement of an adversary force. The obstacles can be natural, manmade, or a combination of both. Obstacles can be used to delay or redirect the advance of personnel, equipment, and vehicles of the adversary force. A barrier is a coordinated series of obstacles than can channel, direct, redirect, delay, and/or stop the movement of an adversary force. Barriers are most effective when they can be used to redirect the approach of adversary forces. They are also employed to prevent adversary vehicles from entering an installation or the area around a critical facility. Barriers may be passive (fences, walls, vehicle barriers, etc.) or active (pop-up vehicle barriers, etc.). Barriers may also be provided by natural elements of the terrain, such as mountains, rivers, thick forests, ravines, etc.

Best Practices for Delay:

- The design of facility delay elements should be balanced to provide equivalent[33] delay times. This also applies to the site delay elements.

- Unattended openings should be protected by delay features that provide delay times that are equivalent to the boundary being penetrated.

- Delay systems and elements should only be installed when complemented with detection and assessment systems. Delay only occurs after detection with assessment and a security response initiated.

---

adversaries who do know how and are skilled at defeating delay elements, thus taking only a short time to defeat the delay elements.

[33]The use of equivalent is not meant to require that *all* delay times be the same. Rather it is used to ensure that no one delay element has a delay time that is substantially less than the delay times for the other elements in the layer. This prevents one path through the layer from being much easier to penetrate. Thus, for example, the doors that penetrate a massive concrete wall do not have to have the exact same delay as the wall, which may be several minutes; rather the delays for the doors that penetrate the wall should be comparable and this delay should be sufficient to ensure adequate response force time when all other protection system delays are considered.

- Multiple and different barriers or combinations of delay elements should be used to provide delay-in-depth and to extend penetration times by increasing adversary task complexity, thereby requiring the adversary to use different skills, better planning, and a variety of tools to defeat the delay.

- The use of active delay systems with passive delay elements are complementary and improve the overall delay effectiveness.

- Delay systems that are installed close to target sets are usually the most cost-effective; however, care must be taken to ensure that this delay cannot be used to make it difficult for the response force to perform its function.

- Barriers, when possible, should be located, designed, and installed so that they do not provide a defensible fighting location for the adversary force.

- Delay incorporates robust facility design features that include gabion wall construction, concrete and earth overburden, and massive delay doors with preferably equivalent delay to walls.

- Delay incorporates advanced response and denial systems or the infrastructure capability to install these systems at a later date should the adversary threat and capabilities increase. Examples of advanced response and denial systems include:

  – Remotely Operated Weapon System
  – Munitions-Based Access Denial System
  – Dispensable materials (e.g., cold smoke, sticky foam)

- Emergency egress is designed such that it does not defeat delay elements.

- Effective delay systems:

  – Limit the number of paths an adversary can take to reach the targets being protected

  – Channel, choke, and expose the adversaries to security force assault[34]

  – Allow for the interruption and neutralization of the attack at all points along adversary path

  – Impede the adversary by increasing his task time with robust delay along limited paths and at critical points

- If extended detection capabilities (i.e., sensors that detect in the owner-controlled area) are used, then installation of vehicle and foot travel impediments should be considered (e.g., large rip rock that makes vehicle and foot travel difficult).

[34]Such systems could include robust delay systems at the protected area boundary that allow the response force to neutralize the adversary there.

4.6.3 Response

Security forces provide the response function. The appropriate design and construction of security force response facilities is critical to ensure timely interruption and neutralization of an adversary attack. Security force facilities are an integral part of the overall nuclear power plant design. The type, location, design, and construction of security force facilities should be well thought out with the design requirements based on comprehensive threat and risk assessments (i.e., the DBT). Security force facility design should also include the capacity to include *future* physical security upgrades and new technology solutions in order to meet higher protection requirements resulting from new threats and increased adversary capabilities.[35]

Security force facilities, which are discussed in the following sections, include central alarm stations and secondary alarm stations, permanent posts, fighting positions, and training facilities. To be effective the response force must know where the adversary is so that appropriate tactics can be employed to defeat the adversary. Situational awareness components such as cameras and motion or sound sensors can be employed to help the security force determine the locations of the adversaries. These components may be in excess of those needed simply for detecting the adversary.

4.6.3.1 Central and Secondary Alarm Stations

A central alarm station (CAS) is essentially a security command center that controls security communications, interfaces with site operations, and is the central point where alarm and assessment information is transported to the AC&D system. A secondary alarm station (SAS) provides a backup system, with redundant capability, for the CAS.

Best Practices for a CAS and SAS:

- The CAS and SAS should be located within a protected area.
- The CAS should be segregated from normal plant operations.
- The CAS may be co-located close to identified target areas but segregated from normal plant operations.
- The CAS and SAS should be hardened to protect against adversary weapons fire and explosives devices as determined by the DBT.
- The CAS and SAS should be equipped with duress systems that annunciate to other security posts.
- The CAS and SAS should be equipped with alternate communication systems.

[35]This requires the designer to consider the need for allowing additional, and as yet unused, space and support (e.g., power and communications) in the design of the security force facility. Simply stated, the design should allow space for future expansion.

- The design of the CAS and SAS should incorporate a positive and separate entry control system with two-person controls to ensure that both personnel and equipment are adequately protected against both insider and outsider threats.

- The CAS and SAS AC&D system should have backup power sources to ensure continuity of operations for a minimum of four hours.

4.6.3.2 Permanent Posts

Permanent posts are designed as fixed positions at optimum locations where security forces control access to a protected area and those areas containing high-consequence targets. These posts include entry/exit control points designed to allow authorized entry/exit of personnel and vehicles. Permanent posts should provide the capability to inspect and search personnel and vehicles, packages, and hand-carried items to deter and detect inbound prohibited and controlled articles and outbound unauthorized removal of other assets. Permanent posts may also include towers, overwatch positions, response vehicle positions, and hardened fighting positions.

Best Practices for Permanent Posts:

- Posts should provide adequate human factors engineering to ensure that security personnel can perform their duties efficiently. Posts should also provide protection from weather and temperature conditions, adequate lighting, and facilities to meet personal hygiene needs. In addition, post design should consider work-related environmental hazards (e.g., lead and carbon monoxide).

- Post design should consider defense-in-depth and redeployment strategies inside the power block.

- Posts must be located such that likely routes of adversary entry and exit or their attack paths can be clearly observed and countered by security force interruption and neutralization tactics (i.e., cover and concealment opportunities for the adversary should be minimized). These posts may take the form of multilevel fighting positions that are built into the appropriate facility buildings. These fighting positions should allow the response force personnel to engage the adversaries before they enter the site, before they enter specific buildings on the site, and within specified buildings. Where possible, these posts should provide for overlapping fields of fire.

- Posts must provide protected routes or avenues of tactical approach by responding security force personnel. For posts protecting the interior of buildings, entry should require passage through an established fighting position.

- Entry/exit control posts must be designed to provide unobstructed views to facilitate observation of unauthorized attempts to bypass detection systems.

- All posts should be hardened to provide security personnel adequate protection against weapons fire and explosives devices as determined by the DBT.

- All posts should be equipped with duress systems that annunciate at a minimum in the CAS and SAS. Annunciation may include other overwatch posts but should not include the initiating post.

- All posts should be equipped with readily available alternate communication systems (e.g., two-way radio fixed-base system, mobile radio systems, telephone, dedicated direct line telephones, intercom systems).

4.6.3.3 Security Fighting Positions

Security fighting positions are generally defensive in nature and are used to provide hardened, force protection positions from which to direct fire at attacking adversary forces. Fighting positions can also be used as observation points, fire control points to direct fire from other positions, or offensive positions that the security forces respond to in an attempt to interrupt and neutralize adversary forces.

Best Practices for Fighting Positions:

- Fighting positions should be designed to take advantage of natural terrain features, site layout and facility design, and target and asset locations.

- Fighting positions should be located such that adversary cover and concealment is minimized (e.g., if a fighting position is located such that the effective field of fire is in a corridor, then the corridor should be kept clear of materials that may be used by the adversaries).

- Fighting positions should provide directed fields of fire for the type of security force weapons used at each position.

- Fighting positions should provide overlapping fields of fire with adjacent fighting positions.

- Fighting positions should be hardened to protect against weapons identified in the DBT.

- Fighting positions placed at the protected area boundary should be designed to allow for surveillance into the owner-controlled area in day/night conditions and should have components to allow for alarm assessment.

4.6.3.4 Training Facilities

Training facilities support security forces and enable these forces to maintain the knowledge, skills, and motivation to effectively perform response functions critical to the protection of high-consequence assets. This includes facilities for weapons and physical fitness training, qualifications, and maintenance; special skills and site-specific training and qualifications; and simulated site target locations for force-on-force training.

Best Practices for Training Facilities:

- Training facilities must be capable of supporting realistic and intense security force training and qualification programs required to effectively engage and defeat a well-armed, trained, and motivated adversary.

- Physical fitness facilities should contain diverse types of equipment to support both musculature and cardiovascular development and maintenance.

- Training facilities should be located on site, or near the site, to maximize training process efficiency and minimize lifecycle training costs.

4.6.4 Insider Mitigation

Insider adversaries have the benefit of having authorized access past standard access controls designed to detect and adversary intrusion. Risk of active or active violent insider actions may be mitigated by an insider mitigation program. An insider mitigation program consists of two parts, elements that mitigate the intent of a potential insider and elements that mitigate the capability of a potential insider. Personnel related programs such as Access Authorization, Behavioral Observation and Fitness-for-Duty address an individual's intent to commit sabotage. The physical protection part or component of a program consists of search devices at personnel access portals, surveillances by security force personnel to identify tampering and specific measures to detect insider actions attempting sabotage at target locations. The remainder of the discussion in this section describes how to develop those measures to identify and develop design elements to detect insider sabotage actions at target areas.

Best Practices for Insider Mitigation:

- Physical protection measures that detect insider acts of sabotage include both physical and administrative controls. An analysis should be performed, specifically focused on active insider acts of sabotage to develop the measures. The first step involves identifying those components or areas that could be potentially vulnerable to acts of insider sabotage and are targets within a target set.

- For example, at a nuclear power plant, a specific type of valve may serve to provide a specific safety function that is relied upon to maintain core cooling and therefore the valve and the mechanisms to control it would be potential sabotage targets. Measures to protect this function could include placing the mechanisms that could control the valve (outside of the control room) in a penetration resistant cabinet that is tamper alarmed and locked. These physical measures could be incorporated into the design of the facility. The design scope would include the physical location of the cabinet, the construction materials of the cabinet, the type of lock, and the conduit pathways that would supply power, and signal information for the valve and the tamper switch. Additional administrative controls for this example could include implementing a two person (i.e., both are knowledgeable persons) rule when such a cabinet is to be accessed, developing key control measures for the lock to the cabinet and developing security force measures that outline the response to cabinet tamper alarm received in an alarm station.

4.6.5 Additional Physical Protection System Considerations

In addition to the best practices identified in the previous subsections, the following best practices are offered:

- Loading and unloading of trucks transporting fuel (i.e., mixed oxide) should be performed in buildings that completely enclose the truck and the loading/unloading activities.

- Sally-port designs for package, personnel, and vehicles should ensure that:

  – Only one portal (i.e., entry or exit) can be open at a time (i.e., one portal is always closed)

  – Security force personnel can direct fire into these areas from fighting positions

  – Over-watch positions for these areas should have emergency lock-down capabilities

- Personnel access and material portals that can be located underground may be used to deny access to the facility through these portals if adversary actions are detected.

4.6.6 Planning for Future Threat and Adversary Capability Changes

Given the current threat environment, a seemingly ever-increasing threat potential, it would be prudent to plan for increases in threat and adversary capability. To this end, nuclear power plant facility designers should consider "designing in" potential upgrade capabilities into a facility design that is to be submitted in a design certification or combined license application to the U.S. Nuclear Regulatory Commission for approval. Examples to consider include:

- excess conduit and conduit channel capacity to allow addition of communications, control, and power cables for additional and/or new detection, delay, and response protection elements

- locations where additional hardened fighting positions can be installed to address increased numbers of adversaries or capabilities

- locations where additional active denial systems can be installed to increase delay and/or increase the potential for neutralization

In addition, the designers should perform sensitivity studies on the proposed PPS design, using the integrated analysis techniques and tools described in Chapters 2 and 3 and increases or changes in the DBT (both numbers and capabilities), to identify the PPS breaking point (i.e., the point at which the PPS no longer provides adequate protection) and to identify potential PPS modifications that if implemented would allow the PPS to prevent the undesired consequences. Once these modifications are identified, the current facility and PPS design should be examined to identify how difficult it would be to implement these modifications. If the modifications can be made with minimal future cost, no additional work need be performed. However, if substantial future cost would be necessary, then the designers should reexamine the proposed PPS to de-

termine whether modifications could be made that would not impact current PPS effectiveness but would facilitate the implementation of the future upgrades.

4.7 Best Practices: Evaluate the Physical Protection System Design

4.7.1 Pathway Analysis

For a pathway analysis to be effective, the person performing the analysis must be intimately familiar with the ongoing or proposed plant/facility design. They must be aware of all credible ways in or out of each location, building, and room. They must be able to think like the adversary and understand how the adversary could:

- use the terrain or local environment to evade detection
- defeat or bypass protection elements using standard or imaginative techniques (i.e., how can they go over, through, around, or under the protection element)
- use deceit or stealth to gain entrance into the facility

4.7.2 Neutralization Analysis

The performance of an effective neutralization analysis requires the use of subject matter experts who are familiar with adversary tactics and those familiar with all aspects of the protection force (e.g., travel time to assigned post once alarm has been sounded, security force deployment tactics, use of deadly force, and weapons deployment). The analysis should consider the variation in possible environmental conditions (e.g., day or night, season of the year, clear or foggy) and how such conditions affect the ability of the protective force to respond to an attack. In addition, the analysts must be familiar with the tools that will be used, especially their weaknesses, to estimate the probability of neutralization.

4.7.3 Risk Analysis

An effective risk analysis combines the information from the other parts of the design and analysis tasks to determine the risk associated with a particular design.[36] In addition, the analyst should be able to identify system weaknesses and understand why those weaknesses occur.

[36]Remember, the typical analysis currently being performed is a conditional risk analysis where an attack is assumed to occur and the objective of the analysis is to determine the effectiveness of the PPS in preventing the undesired consequences. Thus the focus is on determining P_E (i.e., probability of system effectiveness).

5. SECURITY SYSTEM TECHNOLOGIES

5.1 Introduction

As part of the revision to NUREG/CR-1345, Sandia National Laboratories (SNL) was tasked to provide information on a select set of security technologies. While the following sections provide information on the set jointly identified by the U.S. Nuclear Regulatory Commission (NRC) project manager and the SNL staff, the following caution is provided:

> Security technology is a rich and diverse research and development arena. Solutions to the new challenges facing post-9/11 America are works in progress. Some promising new products have been developed recently and are discussed briefly in the following sections, but the reader should note that any discussion of new technology is a snapshot in time. Upgrades, updates, and new directions are inevitable. Security system designers are encouraged to seek advances in security technology that have occurred since this list was compiled in late 2006.

Each technology profiled includes what it does as far as detection, delay, or response and information on what it takes to implement (e.g., cost, footprint, electrical requirements). SNL personnel and others are listed as primary contacts for additional information. In addition, NRC physical security staff may be able to aid in providing more information as well.

5.2 Trace and Bulk Explosives Detection Systems

5.2.1 Introduction

Detecting contraband carried by personnel upon entrance to a facility can be difficult and time-consuming. While a physical search by security officers can be thorough, the process is labor-intensive and slows the throughput for personnel traveling to work.

Using technology to detect explosives can solve many of these problems. Two main technologies, trace and bulk explosives detection systems (EDSs), provide solutions for various detection applications, including the detection of explosives carried by personnel or concealed in packages and vehicles. The purchase of an EDS depends on the application for which it is intended. As with all detection systems, the response to an alarm must be determined by the site using the EDSs. The response to an alarm should consist of a decision tree of actions that may include, but are not limited to, a second sampling for detection, interview of the person associated with detection, isolation of a potential explosive, canine team detection, and expulsion from the site. The user should be cautioned that the best system for explosive detection relies on several diverse methods, such as x-ray, manual search, canine, and trace detection.

5.2.2 Trace Explosives Detection Systems

Trace EDSs can detect explosives residue on personnel, packages, and vehicles from the vapor or particles exuded from bulk explosives that are present or residue left by the handling of explosives. Many of the trace detection sensors, designed to analyze chemicals, can be adjusted to test for illegal drugs rather than of explosives.

For personnel screening applications (Figure 5-1), the dimensions of a personnel portal footprint is approximately 75 in. long by 50 in. wide and 90 in. tall, weighing approximately 1800 lb. Power requirements include access to 208/220 VAC, 50 Hz or 60 Hz, with a 40-amp maximum. Costs for commercial explosives detection personnel portals range from $100K to $150K.

Handheld EDSs (Figure 5-2) can provide mobility that a portal cannot and thus can provide for the inspection of packages and items carried by personnel or shipped to the facility. Commercial handheld EDSs can range from 6 to 12 lb, and the available technology includes ion mobility spectrometry, chemiluminescence, gas chromatography, mass spectrometry, surface acoustic wave, and thermo-redox. Equipment size is approximately the size of a small carry-on bag. Prices range from $20K to $60K, depending on the equipment and its capabilities. Another class of similar equipment includes benchtop or semi-portable detectors that weigh considerably more, from 50 to 165 lb, and range in cost from $25K to $60K. These detectors are suitable for placement at a checkpoint and can be used for checking vehicles or packages via swipe sampling.

Vehicle portals using trace technology are under development as well (Figure 5-3). The footprint is roughly 18 ft by 8 ft by 7 ft and the cost is approximately $200K. The trace portals work by removing a vapor sample from the interior or exterior of the vehicle and detecting trace residues of explosives.

Figure 5-1. Trace explosives detection personnel portal undergoing a test at a Department of Energy facility.

Figure 5-2. An example of a handheld trace explosives detection system.

Figure 5-3. An example of a mobile trace explosives detection vehicle portal.

5.2.3 Bulk Explosives Detection Systems

Bulk EDSs use a radiation source to interrogate the person, item, or vehicle in question and detect and analyze the response from all materials present. In bulk detection, a visible mass of explosives material is detected, either by imaging techniques or through technology that probes nuclear (i.e., elemental and molecular) properties of the material. Bulk explosive techniques measure and analyze the characteristics of the materials in question in an attempt to detect the possible presence of explosives.

While some personnel screening applications have been developed and approved for use (e.g., low-dose backscatter x-ray), the public perception of being subjected to any type of radiation (and the resulting privacy issues associated with imaging beneath clothing) makes the implementation of such types of EDSs problematic. Companies have developed algorithms that conceal the human image while identifying anomalous areas that may indicate concealed weapons or explosives. The footprint for such units is large and may require up to 15 ft by 6 ft (Figure 5-4). The purchase cost can be in the $100K range.

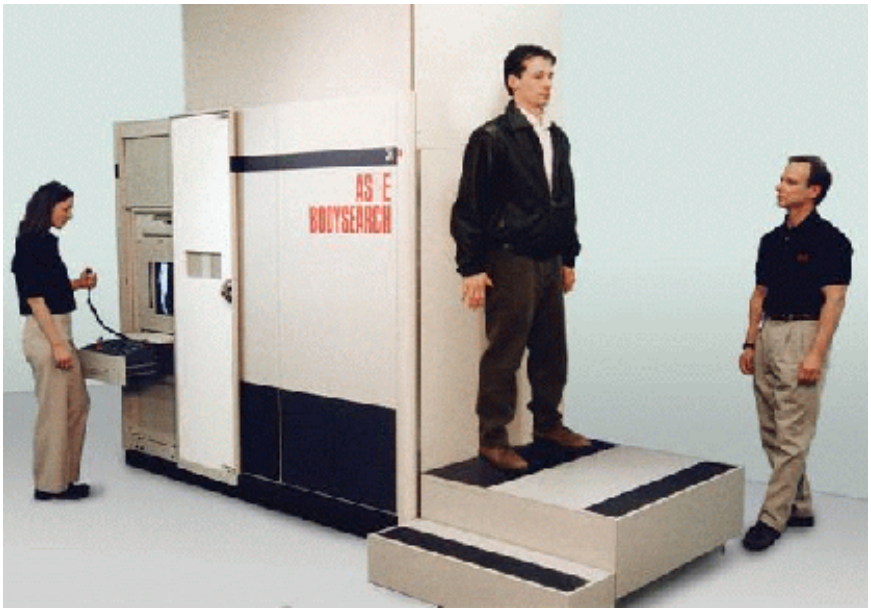

Figure 5-4. Example of a low-dose backscatter x-ray personnel screening system *(Photo courtesy of AS&E)*.

Inspection of items such as packages or bags can be performed with x-ray- or gamma-ray-based EDSs, computed tomography, or some form of nuclear interrogation. This type of technology is mature and is often seen in airports, where travelers place their bags on a conveyor belt. The item is interrogated with ionizing radiation and an operator inspects the image for contraband. This form of detection can be subject to human error and operator fatigue. To combat these issues, commercial vendors are developing software that automatically flag suspect areas for operator inspection. Some computed tomography systems automatically detect molecular weight and quantity of target compounds and generate an alarm, but these devices may cost from $500K to $1000K and require an area 15 ft by 6 ft for installation.

Vehicle screening for bulk explosives can be accomplished in portals that can accommodate large (semi-truck-sized) vehicles and can typically cost from $250K to $500K. However, personnel must exit the vehicle before scanning. One such portal has motorized dual scan heads that move on tracks along each side of the vehicle being inspected, and each scan head has an electronic neutron generator that interrogates the vehicle from the exterior to image the interior. An array of detectors captures the integrating neutrons enabling an image to be formed that may highlight areas of possible explosives.

For additional information contact:

William Rhodes III, Manager
Contraband Detection Dept.
Dept. 6418
(505) 844-4597
wgrhode@sandia.gov

For information about how to purchase EDSs and a complete list of available technology, consult the National Institute of Justice's website for the *Survey of Commercially Available Explosives Detection Technologies and Equipment 2004*, at the following location: http://www.ncjrs.gov/pdffiles1/nij/grants/208861.pdf.

5.3 Vehicle Barriers

The U.S. Department of State publishes a list of commercially available vehicle barriers that have been certified by test as acceptable for use against threat vehicles of 15,000 lb up to speeds of 50 MPH. In the post-9/11 era, the U.S. government has experienced an escalation of the threat level to many of its high-security national assets. With the escalating threat level, these barriers are either unproven or inadequate. As a result of this increase in threat, performance validation testing of vehicle barriers typically used to protect these national assets or facilities has been conducted to determine whether the vehicle barriers provide sufficient delay or denial against the current threat.

This testing program was conducted for a consortium of federal agencies including the Department of Energy (DOE), the Department of Defense (DoD), the State Department, and others. Commercially available vehicle barrier products as well as new collaborative designs were tested, including fixed bollards, fixed vehicle barriers, and hydraulically activated vehicle barriers.

Some of the vehicle barriers in use today at many federal facilities were designed and installed prior to the escalation of the threat level. This testing program provides test data of the barrier performance against a threat several times the design basis of these barriers.

New innovative solutions to prevent vehicle penetrations have been tested for the DoD (Figure 5-5). These barrier designs take advantage of locally available materials to assist in stopping the threat vehicles where large perimeters must be protected. This use of available materials is shown in Figure 5-6.

Figure 5-5. Testing new shallow mount vehicle barrier design

Figure 5-6. Concrete and sand vehicle barrier

Each site or facility to be protected against vehicle threats presents many different design challenges.[37] The shallow mount design pictured in Figure 5-5 was developed by the Texas Transportation Institute and SNL for urban use. There is no typical solution; cost estimates and space requirements are developed on a site-by-site basis. The Delta DSC501 wedge-type hydraulic vehicle barrier (Figure 5-7) costs about $65K installed and requires electricity to power the barrier. The RSA vehicle barrier (Figure 5-8) costs about $1200 per linear foot. Vehicle barrier costs range upward from about $230 per linear foot, depending upon the size and design of the vehicle barrier that provides the required delay.

Figure 5-7. Delta DSC501 hydraulic vehicle barrier.

Figure 5-8. RSA vehicle barrier.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

Mark McAllaster
Vehicle Barrier Testing Lead
Dept. 6422
(505) 845-8349
memcall@sandia.gov

5.4 Remotely Operated Weapon Systems

Recent events have dramatically increased the need for more effective security of high-value assets. Unfortunately, increasing security system effectiveness through traditional means (e.g., more response personnel) is challenged by the need to reduce the cost of security. One possible

[37] As a design note, vehicle velocity may be lessened to meet vehicle barrier kinetic energy capabilities (e.g., use of serpentine approach path), and terrain features may be used to deny access of a vehicle threat. See NUREG/CR-4250, -6190, and other guidance documents on this topic available from the NRC.

solution to the "do more with less" goal is the use of Remotely Operated Weapon Systems (ROWS) (Figure 5-9). ROWS have the potential to offer significant force multiplication and increase response efficiency through improvements in delay and response.

There are numerous advantages to using ROWS as a supplement to a security response force. The primary benefits are instantaneous response, ability of a single operator to respond to threats in different locations, increased target accuracy, immunity from hostile fire, and increased tactical efficiency. Unlike a human, the ROWS does not get fatigued, and its accuracy is not affected by tremor, trigger anticipation, gun recoil, or shooter fatigue. Its accuracies approach and sometimes exceed those of the best human snipers. Because ROWS is controlled remotely by someone who is not in the line of fire (Figure 5-10), better decisions can be made about when to shoot. Other advantages include the ability to respond to multiple threats and locations from one command center; immunity of the system to biological, radiological, chemical, and other environments; and increased firepower with reduced costs.

Figure 5-9. Remotely Operated Weapon Systems platform.

Figure 5-10. Remotely Operated Weapon Systems console.

During evaluations, developmental ROWS systems were installed at SNL locations. Trained operators practiced using them against a variety of threats and scenarios. SNL also modeled the use of ROWS on the Joint Conflict and Tactical Simulation system (a computer modeling and simulation program that can estimate the delay imposed on an adversary through an added security feature). In many of the simulations, ROWS improved the accuracy of the operators and provided additional delay, giving human responders a better probability at stopping or repelling their adversaries.

A ROWS is operated from a remote, secure location and consists of a weapon that is mounted on a robotic platform that can aim and fire the weapon. An operator controls the robot, and thus the weapon, from a remote location by using a joystick and is able to view potential targets on a

video screen that displays exactly where the weapon is aimed. For safety, two people are required for operation of a ROWS. Numerous safety features have been incorporated into the system to make accidental discharges nearly impossible.

These platforms have the advantages of exceptional targeting accuracy, using a suite of optical and infrared cameras for surveillance and targeting. With the addition of video motion detection, these cameras also could be used with as an area intrusion sensor. The Generation 2 T-250FS model can accommodate the M16, M240, M249, and .50-caliber sniper weapons.

The tactical platforms have proven to be robust and easily handled. With the .50 caliber weapon option, the platform could potentially protect assets out to 1000 m or more. They could be used to provide protection for critical infrastructure, pipelines, bridges, and other areas where the potential for ambush or sabotage is high.

The hardware costs for the platform are in the range of $250K per unit. The first-time installation cost, which includes infrastructure, safety analysis and reviews, training, maintenance program, and the like, is about $1M per platform. The platform requires mounting, tower construction (for exterior applications), power, and fiber optic signal lines. A command and control console is also required.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

5.5 Advanced Concept Armored Vehicle II

The Advanced Concept Armored Vehicle II (ACAV II) project, funded by the Department of Energy Office of Security and Safety Performance Assurance, studied requirements for mobile armored platforms, developed specifications, and researched methods to incorporate commercially available technologies to produce an advanced armored vehicle that met the needs of asset protection (Figure 5-11). The ACAV II took advantage of new armor developments and other technologies to field a vehicle similar in cost to currently used armored vehicles. The ACAV II is a Class VI vehicle with thermal and closed circuit television (CCTV) viewing for the driver and a platform equipped with a thermal scope, standard scope, and CCTV for the gunner. As of 2006 the ACAV II can mount M-16s, SR-25s, M-249s, and M-240s. The gunner is not exposed and the weapon utilization is remote. The weapon is housed in a metal enclosure in the bed of the vehicle (Figure 5-11). The controls can raise and lower the weapon and provide continuous 360-degree travel horizontally and 60 degrees of elevation.

Figure 5-11. Advanced Concept Armored Vehicle II production armored response vehicle.

Figure 5-12. Advanced Concept Armored Vehicle II prototype with weapon aiming and surveillance platform.

The ACAV II uses a long bed, one-ton pickup. Two ACAV II variants have been developed:

- 2004 General Motors Corporation ¾-ton 2500 Sierra pickup truck (converted to 1 ton). The vehicle's engine and transmission are an extremely efficient and reliable combination that provides for sufficient power from a standstill position, noticeably more than that provided by the Ford F-350's engine and transmission combination.

- 2005 Ford F-350 (1-ton) Super-Duty 4x4 pickup truck (production variant). This vehicle design facilitates adding a door hinge to each door, which can be expected to significantly increase the operational life expectancy of the armored doors.

Each of these weighs approximately 10,000 lb when fully equipped. The ACAV II is self-sufficient and requires no external power. In addition to providing a stronger response, the ACAV II is equipped with surveillance cameras, which can be used on patrol to augment detection capabilities. Delay is also added by the stronger response.

The cost to outfit the base vehicle is approximately $160K, which is comparable in cost to the armored vehicles now in use. Adding weapons brings the total cost per unit to approximately $300K.

For additional information contact:

Jack Jones
Transportation Assessment Department
Dept. 6454
(505) 845-9867
jacjone@sandia.gov

Skip Metcalf
Transportation Assessment Department
Dept. 6454
(505) 844-7879
hemetca@sandia.gov

5.6 Virtual Presence and Extended Defense

A Virtual Presence and Extended Defense (VPED) system extends detection, assessment, and possibly delay beyond traditional perimeters, so response forces have earlier warning of adversary attacks or surveillance. It places sensors and assessment beyond a site (i.e., protected area) perimeter to detect adversaries farther out (i.e., in the owner controlled area). The advanced warning provides response forces more time to respond to the threat. The VPED system is designed to detect personnel and small vehicles along specific avenues of approach or assembly areas (e.g., a ditch or draw that allows adversaries to approach an owner-controlled area with little likelihood of being seen by a roving patrol or a position that could be used by an adversary as a sniper position) and is not intended to be used to create a fully sensored extended perimeter (see Figure 5-13).

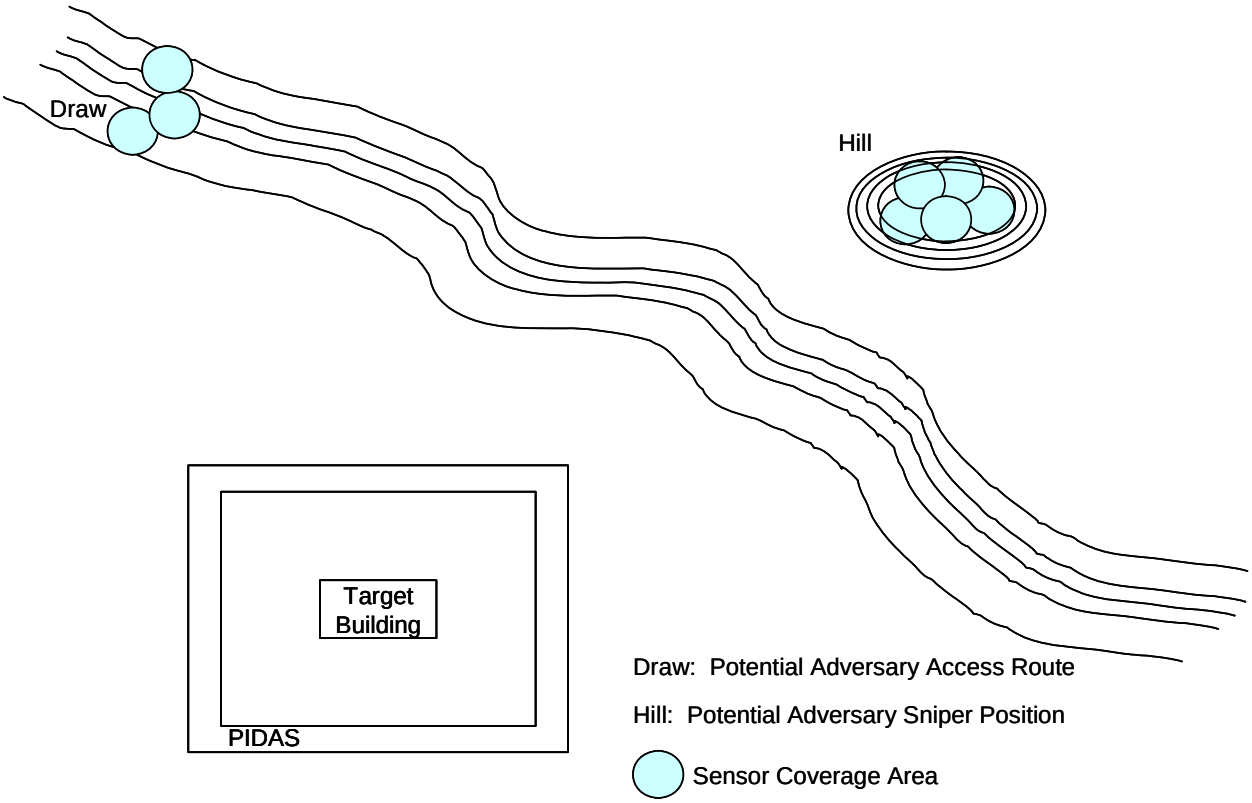

Figure 5-13. Notational diagram of site with potential adversary access route and sniper position instrumented with Virtual Presence and Extended Detection system sensor nodes.

A VPED system is not designed to replace a traditional Perimeter Intrusion Detection and Assessment System (PIDAS), but rather to augment an existing PIDAS to give better security system effectiveness for land-based assault scenarios (i.e., foot and/or vehicle assaults).[38] The VPED system consists of low powered sensors, and optimal performance of a VPED system is achieved when sensor and assessment systems are tuned to maximize their performance in the deployment terrain. Tuning requires a period of monitoring and adjustment. Tuning times for a VPED system are currently a few hours to a few days during initial system installation.

The current VPED system consists of sensor nodes (Figure 5-14) that support sensor transducers and cluster nodes (Figure 5-15) that provide video assessment capability. Both sensor and cluster nodes use radio frequency links to send data to a command center and provide 360-degree

[38]Because a VPED system is typically deployed in a natural (i.e., unengineered) environment, the system, at any one sensor, may experience a higher than usual nuisance alarm rate when compared to the rate from a sensor in a PIDAS where the environment has been engineered. Therefore a VPED system is normally installed only for those locations where advance knowledge of a potential threat incursion is worth the higher nuisance alarm rate or may be installed and subsequently used only during heightened states of security awareness when a higher nuisance alarm rate is acceptable.

field-of-view coverage. Sensor nodes are self-powered using internal batteries and can operate for more than two years on internal power. Cluster nodes are powered by solar panels and provide both day and night assessment and sensor fusion capabilities.

Figure 5-14. Virtual Presence and Extended Detection sensor node.

Figure 5-15. Virtual Presence and Extended Detection cluster node.

A VPED system also includes software to help reduce nuisance alarms, also known as the nuisance alarm rate (NAR). Four technologies are used to reduce the NAR:

- intelligent senor algorithms that attempt to classify detections as persons, vehicles, or other
- sensor fusion that combines multiple sensors to provide more accurate detection
- video assessment to allow operators to determine the cause of a detection notification without having to dispatch patrols
- a user interface that can be operated effectively under high sensor alarm conditions

These techniques help a VPED system reduce NAR to levels that make beyond-the-perimeter sensor systems effective despite their deployment in unconstrained external environments (where administrative measures, i.e., controls, are not effective).

The VPED system has its own stand-alone user interface for users without a command and control system. The VPED user interface is web browser-based and can be deployed quickly almost anywhere on a user's network. For users who do have a command and control system, VPED is designed to work with other display systems through standard network interfaces such as XML. The VPED system can be quickly customized to work with most modern network-based command and control systems.

VPED equipment was prototyped in 2005 and in 2007 a second-generation system was deployed in several field applications to validate system operation.

For additional information contact:

David Kitterman, Manager
Virtual Presence and Extended Defenses Department
Dept. 6428
(505) 844-6853
dlkitte@sandia.gov

5.7 Long Range Acoustical Device

The Long Range Acoustical Device™ (LRAD®) is a hailing, notification, and warning system produced by American Technology Corporation (ATC). The LRAD® 1000 system is shown in Figures 5-16 and 5-17. The LRAD® uses a piezoelectric transducer phase array to produce a narrow 30-degree acoustical beam that can effectively project intelligible speech out to approximately 300 m over land and warning tones out to approximately 600 m. A VoxTec International Phraselator® can be utilized with the LRAD® to provide selectable warnings and instructions that have been translated into a multitude of different languages.

Figure 5-16. Long Range Acoustical Device™ 1000 law enforcement use *(Images courtesy of American Technology Corporation)*.

Figure 5-17. Backside image of Sandia National Laboratories' ATC Long Range Acoustical Device™ 1000 evaluation system showing the simple control interfaces.

The LRAD® provides a cost-effective means to remotely assess, deter, and establish the intent of unidentified/unauthorized personnel approaching or entering restricted areas. With positive determination of intent established, the use of greater force and lethality can be exercised.

The LRAD® 1000 weighs approximately 65 lb, has a diameter of approximately 33 in., and requires less than 400 W at full power output. A typical unit cost is approximately $35K. In addition to the manually aimed system shown, ATC has integrated the unit with the Common Remotely Operated Weapon System, a platform that allows different devices to be installed and controlled, and plans to offer its own pan/tilt unit with remote command and control.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

5.8 Sticky Foam

Sticky foam is a multi-component polymeric resin dissolved in a solvent. When the solution is deployed, a low-density foam is formed that is capable of inhibiting movement and obscuring the object it covers from view. A number of formulations of non-hardening sticky foam have been developed for security applications, including an acrylic-based sticky foam with a broader temperature range of use and superior solvent resistance.

The sticky foams have expansion ratios ranging from approximately 20:1 to 60:1 depending on the formulation and temperature. The foam density depends on formulation, temperature, and dispensing technique and varies from about 1.2 to 3.5 lb/ft^3. The volume stability of dispensed sticky foam depends primarily on formulation and temperature. Volume stability ranges from about 30 minutes to greater than four hours with the reduction in volume less than about 30%. Because the foam is non-hardening, it collapses after a period of time. The material is aggressively tacky and becomes tougher when collapsed.

Sticky foam can be a very effective active delay component of a physical protection system. The intent of the use of sticky foam is to foul tools and to cause intruders to become entangled in the foam and stick to themselves and their equipment. Figures 5-18 and 5-19 show two photos in which an attacker attempts to remove a sticky foam-covered item. These photos demonstrate both the elasticity and the tenacity of the sticky foam material. Using it in combination with other barriers such as tie-downs, cables, barbed steel bands, and other deployable barriers can enhance the effectiveness of sticky foam. Sticky foam provides significantly increased delay effectiveness.

The rubber-based sticky foam material costs approximately $\$10/ft^3$ of volume to be filled. The acrylic sticky foam is nearly twice the cost of the rubber-based sticky foam. The dispensing system cost depends on the dispensing technique used. Sticky foam systems can be either very simple passive systems activated by the adversary's attack or sophisticated activated systems requiring complex command and control systems and dispensing hardware. Thus costs may range from $\$67/ft^3$ of dispensed sticky foam for a fairly simple system to $\$1{,}600/ft^3$ of dispensed expanded material for an activated system. This does not include the cost of the Command and Control system for the activated system. The dispensing system cost may be decreased with additional development and quantity fabrication. Production dispensing hardware also exists.

Figure 5-18. Attacker attempting to remove object covered in sticky foam.

Figure 5-19. Attacker attempting to remove object covered in sticky foam.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

5.9 Obscurants and Deployable Barriers

Activated dispensable materials (see examples in Figures 5-20 through 5-22) are generally used to augment other barriers to deter, delay, or disrupt adversaries. These dispensables can be used to physically impede an adversary or to physiologically interfere with an adversary's sensory inputs, such as obscured vision, olfactory irritants, and impaired hearing. Examples of these dispensables include sticky foam, rigid foam, aqueous foam, visual obscurants, and a variety of irritant and inflammatory chemicals. For access delay applications the deployment of these materials is designed to be non-lethal; however, several of the dispensables can be high penalty in terms of cleanup and safety risk and must incorporate a high-reliability command and control activation system. Activated dispensable delay technologies can significantly increase overall access delay when used in conjunction with substantial passive barriers.

Figure 5-20. Deployable barriers.

Figure 5-21. Cold smoke fogger.

Figure 5-22. Caltrops and sticky foam.

Dispensable materials can be used to complement passive structural-type barriers to defeat or to delay adversaries. Dispensables can be broken into two broad classes based on their function. These classes are 1) entombing and blocking materials and 2) sensory-interfering materials. Deployable barriers are objects such as caltrops and barbed steel bands that can be used alone or in combination with other dispensable materials to provide a synergistic delay effect. Considerations regarding their use in access delay applications include cleanup, toxicology, safety, command and control, and waste.

Sensory-interfering materials make up the second general class of dispensable materials. They include obscurants such as cold chemical smoke, terephthalic acid, pyrotechnic smoke, glycol/water and mineral oil fogs, and aqueous foam. Sensory irritants and inflammatory agents like the riot control agents ortho-chlorobenzylidene malononitrile (CS) and oleoresin capsicum (OC) respectively, are also included in this class of dispensables. Obscurants are effective because they reduce an adversary's vision. This forces him to take additional time to figure out what he must do to succeed. Obscurants also force the adversary to be more cautious so as not to accidentally injure fellow team members. Finally, additional adversary task time is consumed troubleshooting equipment problems that arise on the scene and improvising solutions. The delay effectiveness of the visual obscurants also depends upon the task to be performed. The effectiveness increases as the level of eye-hand coordination required to perform the task increases.

Aqueous foam is not only a visual obscurant; it is also effective against infrared-imaging devices. Aqueous foam attenuates sound and restricts conversation among adversaries. Communication between adversary team members is a vital function if any unforeseen obstacles or complications arise during the adversary attack. However, with advances in portable radio transmitters, it may not be possible to totally mask oral communication between properly equipped persons.

Sensory irritants and inflammatory agents can be used with the obscurants and in some cases, mixed and dispensed simultaneously. Irritants are effective because they force the adversary into protective clothing and breathing equipment. The effect of these agents upon humans is either

temporary incapacitation or physical encumbrance, depending upon whether or not personal protective gear is worn. The desired effect is temporary incapacitation.

Deployable barriers are normally deployed in conjunction with other dispensables for effective delay. The combined delay effectiveness can range from moderate to high. The cost for simple devices can be as low as $2 to $5 each for caltrops, whereas complex devices such as a concertina portcullis (i.e., a downwardly deployable wall of concertina wire) can cost approximately $250K. Design costs are not included.

When multiple dispensables are used in combination in fixed-site protection systems, there can be a synergistic effect on the delay they provide; that is, the delay increases by a factor greater than the sum of the individual delay factors.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

5.10 A Munitions-Based Access Denial System

A Munitions-Based Access Denial System (MBADS) provides lethal denial capabilities to facilities with high-value assets (Figure 5-24). The MBADS utilizes conventional shotgun-style ammunition to provide a wide zone of lethal fire. Multiple units can be covertly placed within a facility at doorways and in hallways. They also can be situated to provide complete cross-fire floor coverage of an entire area.

The MBADS development project leverages technology developed in the ROWS program by using the System Enable Disable Switch (SEDS) function technology to enable the system activation. The SEDS technology relies on mechanical switch contact closures to enable the system, thus eliminating the need for costly software-driven command and control systems to activate the MBADS.

A fire set has been designed to provide timed sequential triggering of ten volleys of shotgun munitions. The delay times between volleys can be pre-programmed to provide time-delayed lethal fire into the targeted area. The time-delayed firing sequence provides both extended access delay times as well as laying down a zone of lethal fire around high-value assets.

The Command and Control station (Figure 5-24) for MBADS is located away from the firing unit in a secure location. The system is remotely fired. It is a standard electronics console about 24 in. wide, 36 in. deep, and 60 in. high. When oriented in the vertical position, the MBADS firing unit is about 12 in. by 12 in. by 84 in. long. It weighs approximately 325 lb. The firing unit can be mounted vertically or horizontally on the wall or can be suspended from the ceiling. It can be installed behind sheetrock or thin wall coverings or hung above suspended ceiling tiles for concealment and surprise attack.

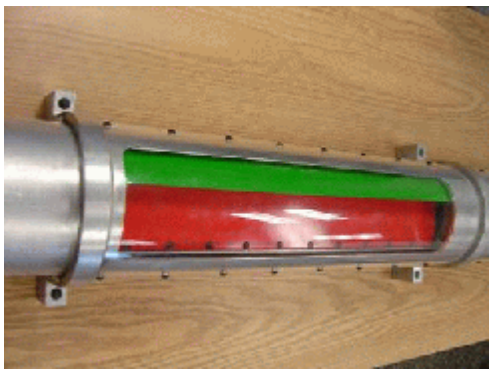

Figure 5-23. Munitions-Based Access Denial System, shield opening.

Figure 5-24. Munitions-Based Access Denial System (MBADS) command and control system, fire set, and MBADS assembly.

The command and control system requires two 120-V, 60-Hz, 20-amp circuits. The same power is also required by a control box in the room where the firing unit is located.

The hardware cost to field one command and control system and eight MBADS firing units is $315K. Seventy rounds per unit can be fired. This cost does not include infrastructure upgrades to any site installing the hardware; neither does it include any Safety Certification cost. A total system cost is typically several times the cost of the hardware alone.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

Mark McAllaster
MBADS Project Lead
Dept. 6422
(505) 845-8349
memcall@sandia.gov

5.11 Gabion-Filled Walls

Thick, heavily reinforced walls can be penetrated fairly quickly using explosives. One alternative that has been proposed to provide additional delay is gabion-filled walls (Figures 5-25 and 5-26). These consist of an outer wall and an inner wall, with the space between them filled with loose rock. The intent of using the gabion material is to form a self-healing wall that will refill

the hole created in the wall by each successive attack. If an adversary penetrates the outer wall, he has to remove a large amount of rock before he can penetrate the inner wall. As he does so, additional rock from above will fall down to fill the hole he is excavating (Figures 5-27 through 5-29).

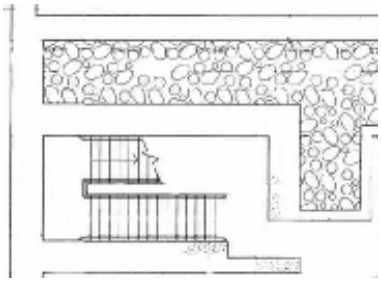

Figure 5-25. Gabion wall in stairwell.

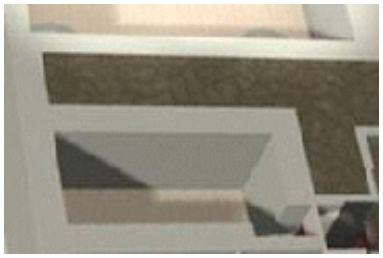

Figure 5-26. Gabion wall in stairwell.

Figure 5-27. Prototype gabion wall construction showing small rock flowing easily through rebar.

Figure 5-28. Prototype gabion wall construction showing large rock does not flow easily through rebar or small holes.

Figure 5-29. Typical gabion fill.

One-tenth scale-model tests of gabion-filled walls were conducted at SNL to gain insight into the behavior of these walls.

Some of the considerations in designing gabion walls include the thickness and height of the walls and gabion fill, size of rock, whether the rock is rounded or crushed, the effect of rebar in the walls on gabion removal, whether there is room for the adversary to remove enough rock to reach the second wall, whether the rock will flow out of a hole in the wall on its own or if the adversary has to work to remove the rock, the cost of construction, long-term compaction and settling, angle of repose of the fill material in the wall and as it flows through a hole in the wall, and so forth.

Gabion walls work best in enclosed hallways, stairwells, small rooms, areas with low ceilings, and other small confined areas where there will be more fill material than available space for the adversary to drain it into. Gabion walls are less effective as exterior walls, in large rooms, or areas with high ceilings.

It is better to make the adversaries work to remove the rock, rather than having it drain itself. Large rock, thick walls, heavy rebar reinforcement, large amounts of fill material, and small volumes to drain the rock into are all more desirable.

It is possible that gabion walls provide an additional benefit of reducing the effect of blast or other aggressive attacks. Because the two walls are separated by a space, this serves to decouple the two walls, so that the shock from an explosive event does not couple as well into the second wall. The intervening space and fill material may help to protect the second wall from robust explosive attack tools. This has not been verified through performance tests.

In designing a facility it is important to have a balanced design that makes all adversary attack paths into the facility equally difficult, either by their construction, location, confined working space, presence of response forces, or other design features. Often the doors, ceiling, floors, and utility chases are much weaker than the walls. If a gabion wall design or other design features make the walls very robust, careful consideration should also be given to these other attack paths.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

5.12 Blue Force Tracking with TacNet (Situational Awareness)

The Tactical Network (TacNet) is a wireless *ad-hoc* self-forming, self-healing network based on Motorola's Mesh Network technology and SNL-developed tracking application software.[39] It provides connectivity between agents (Blue Force) and convoy vehicles for seamless message transfer and situational awareness. The TacNet infrastructure is scalable from a full vehicle convoy awareness system to an in-field tracker-to-tracker system as required.

TacNet improves response force effectiveness by identifying friend and foe, providing situational awareness, and adding a whiteboard capability. In-vehicle displays (Figure 5-30) with a whiteboard allow Tactical Commanders to view a convoy and assets and place, move, and remove icons for good guys, bad guys, etc. Others in the network will also see these icons on their electronic maps. For an in-vehicle system, the TacNet module must interface with the vehicle communications system via a router. Trackers in the field enable response forces to see on their electronic maps their team mates, their vehicles, and any icons placed on the map by the Tactical Commander. For a system of trackers sending data to a control center, the interface must have a router for wireless communications. For tracker-to-tracker communications, the trackers can run as stand-alone units.

Detection can also be provided if the tracker is integrated with radar detection.

Trackers are about 9 $in.^3$ in volume and can fit in standard response force clothing pockets. TacNet Vehicle Modules are about 8 in. by 9 in. by 4 in. (Figures 5-31 and 5-32). The in-vehicle unit cost is $3K (plus $0.5K for a transceiver card). TacNet with display is $1.2K (plus $0.5K for a transceiver card). Without the display, the TacNet is $0.8K.

For additional information contact:

Loren Riblett
TacNet Project Lead
Communications Systems
Dept. 6452
(505) 845-8841
lerible@sandia.gov

[39]Motorola, Inc. developed the MOTOMESH™ Multi-Radio Broadband Solution that allows the deployment of a single wireless network that provides both Wi-Fi access and separate, dedicated and secure access to mission critical communications. Each MOTOMESH™ access point contains two standards-based 802.11 (Wi-Fi) radios and two of Motorola's Mesh Enabled Architecture (MEA®) mobile broadband radios. One set of Wi-Fi and MEA® radios operate in the unlicensed 2.4 GHz band, and one set operates in the licensed 4.9 GHz public safety band. MEA® radio users leverage Motorola's Multi-Hopping® capabilities, turning each user into a router/repeater. Thus MOTOMESH™ access points can be reached by hopping through other users, and each additional user makes the network stronger—extending network coverage and creating more data paths through the network. With the appropriate tools and software, users of the network can receive instant access to information such as data, voice, and video. As with all MEA® radio systems, fast and accurate tracking capabilities are available without the use of global positioning system satellites.

Figure 5-30. TacNet display on map in vehicle.

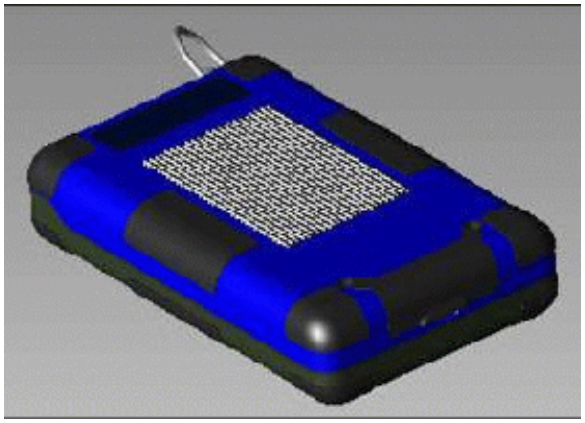

Figure 5-31. Outer view of tractor.

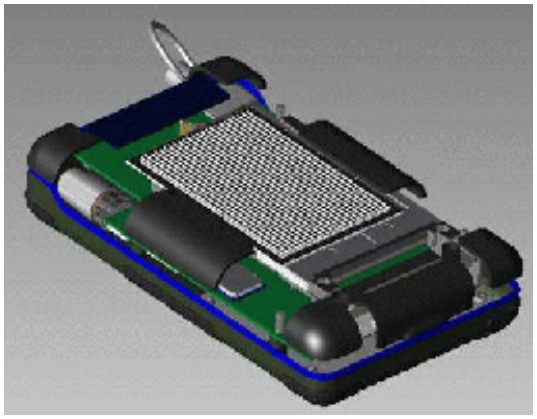

Figure 5-32. Tractor with layers removed.

5.13 Underground Storage and Production Facilities with High Security Doors

Subsequent to the events of September 11, 2001, the DoD revised its directives for munitions storage and production facilities for high-value assets. The revised directives require consideration of all threats, extensive use of active and passive denial systems, and advanced electronic security systems. These DoD requirements emphasize detection, delay, and denial; consequently SNL has employed a synergistic approach to underground facility design using delay, denial, and detection systems working together to produce a deterrent greater than the sum of individual components (Figure 5-33). The SNL design approach also attempts to use normal architectural layout and design features to achieve layered and enhanced delay/denial/detection with minimal added cost.

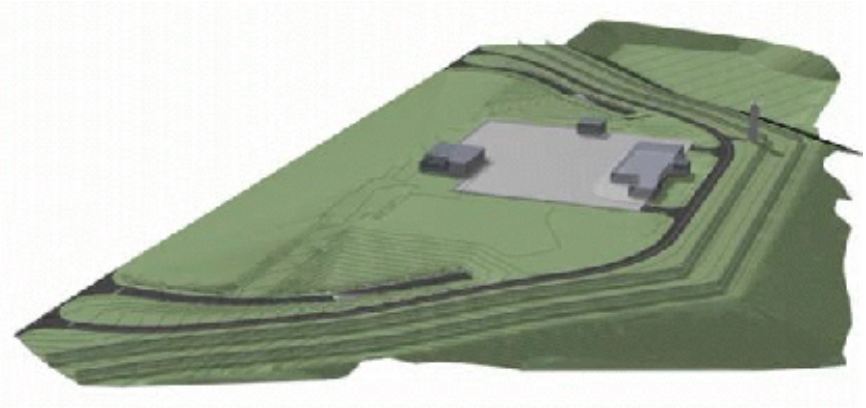

Figure 5-33. Aerial view of buried complex concept.

Addressing air threats is a complex technical issue; SNL has accomplished detailed numerical analyses using its super-computing facilities to develop a mix of energy-absorbing materials to meet the new design requirements for aerial protection of storage and production facilities. Recent explosives impacts testing performed for the DoD at SNL facilities have verified SNL's design effectiveness.

To increase the delay and denial capabilities of underground facilities, SNL has carefully integrated ROWS and MBADS technologies (discussed in Sections 5.4 and 5.10) into areas of the facility design where adversarial forces are either temporarily stopped or channelized and the deadly force attributes of these weapon platforms are maximized. Locating multiple ROWS in series along curved underground facility vehicle tunnels affords overlapping fields of fire, weapon platform protection from stand-off hostile fire, containment of small arms fire from the ROWS, and a highly effective killing zone in front of each gun because the tunnel provides no natural concealment to an adversary. Similarly, MBADS are located at facility entry control points where foot-mounted adversary forces are canalized and can be effectively stopped before reaching critical storage areas.

The entry doors to any secure storage and production facility typically represent the weakest and most vulnerable point in the facility for an enemy attack. SNL working with industry developed high-security doors to meet aggressive adversarial attacks as defined in the new DoD standards thus enabling a balanced facility design from a delay-deny perspective. The performance of the new high-security doors has been validated in testing conducted at SNL and manufacturer facilities for the DoD. The areas immediately surrounding each high-security door are equipped with access delay features to match the delay/denial characteristics of the high-security doors.

In front of the high-security doors, ROWS are positioned to engage adversary forces and bring them under duress during attempts to defeat the high-security doors. Behind the high-security doors (on the secure side), hardened fighting positions are integrated into normal facility partition walls; the hardened fighting positions provide a critical line of defense using an architectural feature of the facility. Delay and denial in-depth are further layered into the facility design by incorporation of high-security control of required blast doors entering storage zones within the facility; blast doors, by design, are robust enough to offer some delay/denial if door openings are controlled.

Currently SNL is working to develop automated alarm, control, and display and entry control systems for control and monitoring of authorized personnel in the most sensitive reaches of the complex. These systems will accomplish a check of personnel identities, Personnel Reliability Program status, shift code, areas of authorized access within the facility, tracking of personnel in critical areas, and control of active denial systems.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

5.14 Smart Camera and Three-Dimensional Video Motion Detection and Assessment

5.14.1 Smart Camera

The Smart Camera is a stand-alone, high-end, digital video surveillance system that uses standard PC microprocessor and local area network technology (Figure 5-34). The embedded microprocessor (within the camera module) allows automated preliminary scene analysis and alarm/notification-level decision-making, which lowers false alarm rates and reduces the amount of operator interactions. The camera's on-board storage buffer captures approximately 120 seconds of full motion video that can be accessed for alarm assessment.

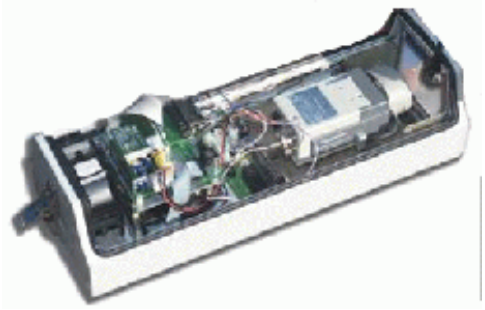

Figure 5-34. Prototype smart camera.

The Smart Camera technology provides many advanced features over traditional analog closed-circuit television systems, including:

- encryption and authentication for control and video data communications between camera module and host/viewer computer, which prevents spoofing and makes the system tamper-proof
- multiple-user viewing and control capability
- remote software modification and update capability

- robust system maintenance tools
- loop recording or instant replay capability
- application programming interfaces for ease of system enhancement or modifications by end users or third-party providers
  - digitally enhanced features, including
  - object recognition
  - scene analysis
  - intelligent alarm processing
  - remote camera tilt, pan, and zoom

The smart camera can be deployed in a wireless configuration and with encryption authentication control and other advanced features can provide significant advantages over conventional camera systems. Figure 5-35 shows a prototype smart camera with an encrypted 802.11 link and 80W solar power system.

Figure 5-35. Prototype solar powered smart camera with wireless link.

For additional information contact:

Virgil Kohlhepp
Advanced Communications and Signal Processing Group
(925) 424-4486
kohlhepp1@llnl.gov

The Smart Camera has been applied in conjunction with another breakthrough technology, the Three-Dimensional Video Motion Detection (3DVMD) and Assessment system described below.

5.14.2 Three-Dimensional Video Motion Detection and Assessment

The 3DVMD system is a stand-alone sensor system that operates on a single PC platform and uses multiple cameras to monitor activity in predefined, three-dimensional volumes of space (Figure 5-36). Detected activity is displayed on the PC monitor as an overlay to real-time video imagery. The basic sensor can provide switch closures for an interface to an alarm communication and display (AC&D) system. High-level detection information relating to the size, location, and direction of motion of moving objects can be provided for assessment purposes. Using this high-level information, 3DVMD can be used to monitor individual items as well as track people within the monitored area. It can be used for two-person rule verification, process control, and the detection of anomalies during evacuation procedures. Specific applications within nuclear power plants could include monitoring mixed oxide fuel assemblies after delivery, utilization as a sophisticated tamper indication device for sensitive component areas, and as a video motion detection system for surveilled areas that will alleviate the necessity for an officer to watch a video terminal with a far less nuisance alarm rate than conventional video motion detection. The 3DVMD system can be implemented as an interior or exterior sensor.

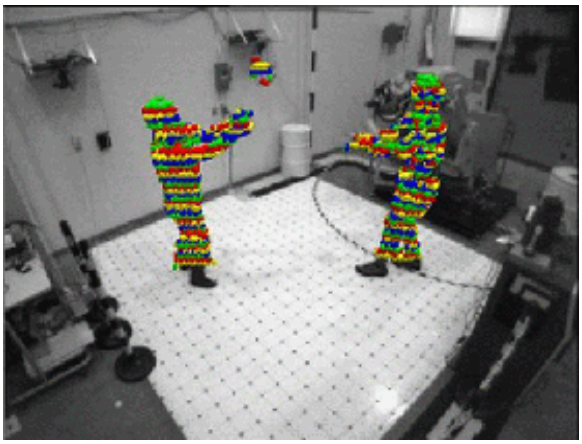

Figure 5-36. Interior monitoring: high-resolution detection of multiple people tossing a ball.

There are several benefits to the 3DVMD technology. It is a passive security sensor. It provides high-level information (e.g., location, size, direction of motion) that can be used as an assessment aid in CCTV video, where it is often difficult to even see an intruder. Its detection volume is user-definable and remains static until changed by the user. This reduces vulnerabilities introduced by the variable detection envelope of other sensors. It has reduced nuisance and false alarm rates as compared to traditional two-dimensional video motion detection sensors. The technology also has built-in redundancy. If a camera fails, the system can adjust to operate without that camera, down to a minimum of two cameras. A 3DVMD system also has a self-assessment (i.e., state of health) capability. Because CCTV sensors are an integral component of the 3DVMD system, the failure of or tampering with any CCTV sensor is immediately identified.

The 3DVMD technology can be fielded either as a stand-alone security system or as part of an integrated security system that provides switch closures to an existing AC&D system. Minimal software development is required to customize the technology for specific applications.

The 3DVMD system has been tested in both interior and exterior environments [Ref. 13]. It has been demonstrated to monitor individual items and to monitor multiple volumes, each with a different level of alarm status. The technology provides assessment information, which generally is not coupled with detection in a sensor system. The assessment data is immediately available to an operator, allowing critical decisions in a timely manner.

The baseline 3DVMD system is a stand-alone sensor system that operates on a single PC platform. The sensor uses multiple cameras to monitor activity in predefined, 3D zones or voxels.[40] The 3DVMD sensor technology was developed for detection and assessment in security applications. It provides high detection capabilities with a low nuisance alarm rate. It is based on the input from multiple cameras and relies on a user-defined volume of space for monitoring. The 3DVMD technology provides significant high-level information about activity within a monitored volume that can be used for assessment information and for input to further processing for more advanced security applications. The developed technology is video-based, but it is **not** a system that requires continual viewing by a human operator. The high-level information can be used to specifically define and extract the activity that would cause an alarm condition. Minimal software development is required to customize the technology for specific applications.

Hardware cost depends on the cameras and central processing unit (CPU) chosen. Cameras range from about $300 to $3000; their selection depends on the application. A CPU costs about $2000 to $4000, again depending on application. Framegrabbers are required if analog cameras are used. A network switch is required if network cameras are chosen. The coverage area is user-defined. The footprint for system componentry depends on the placement of cameras (for example, on towers or mounted on walls). The CPU is the size of a small computer. Power is required to operate the cameras and the CPU.

For additional information contact:

Cynthia Nelson
Virtual Presence and Extended Defenses Department
Dept. 6428
(505) 844-9493
clnelso@sandia.gov

5.15 Automated Screening Systems

5.15.1 Automated Access Control

Automated access control includes accomplishing several functions:

[40] A voxel (VOlume piXEL) is a 3D pixel representing a quantity of 3D data just, as a pixel represents a point (or points) in 2D data.

- identity verification – an authorized person must possess a valid ID card, key fob, or personal identification number

- personnel verification – some form of biometric is used to verify that the person holding/possessing the ID is indeed the person he or she claims to be

- anti-piggybacking – detection and prevention of an authorized person from intentionally bringing in an unauthorized person with him

- anti-tailgating – detection and prevention of an unauthorized person from entering a facility by taking advantage of an authorized person's entrance

- anti-passback – detection and prevention of a weapon or other contraband being passed from outside a facility into the secured area

Several commercial products have automated these functions such that security personnel are not needed except in the event of an exception (i.e., lost ID card, visitor, etc.). These products are usually a set of revolving doors or an enclosed portal (see Figure 5-37). Identity and personnel verification are fairly standard or may be easily customized for a particular facility. Software algorithms that use data from either photo cells or cameras also prevent piggybacking, tailgating, and passback in some of these products. The latest advances in this area involve the use of what is commonly referred to as stereo vision, where the feedback from two cameras looking at the same scene allow for sophisticated determination of the number of people trying to enter the facility—much as a person's two eyes allow for depth perception.

Figure 5-37. Commercially available access control revolving door system.

The footprint of these automated access portals can vary between roughly 3 ft by 3 ft up to 7 ft by 7 ft. Depending on the type of doors used (such as revolving, sliding, etc.), most units will require 110 and 220 power. Maintenance tends to be minimal—a thorough cleaning and/or greasing of the mechanism one to four times a year. These units range in price from $60K to over $100K each.

For additional information contact:

Mary Green
Security Systems and Technology Center
Dept. 6461
(505) 284-5424
mgreen@sandia.gov

5.15.2 Automated Metal/Weapon Detection

Automated metal or weapon detection incorporates a standard metal detector in a portal such that a person entering an enclosed portal booth will be instantly alerted if metal has been detected. That person must then exit the portal through the same door they entered. If no metal is detected in the portal, the person is allowed to exit the portal through a second door that leads into the secured area (see Figure 5-38).

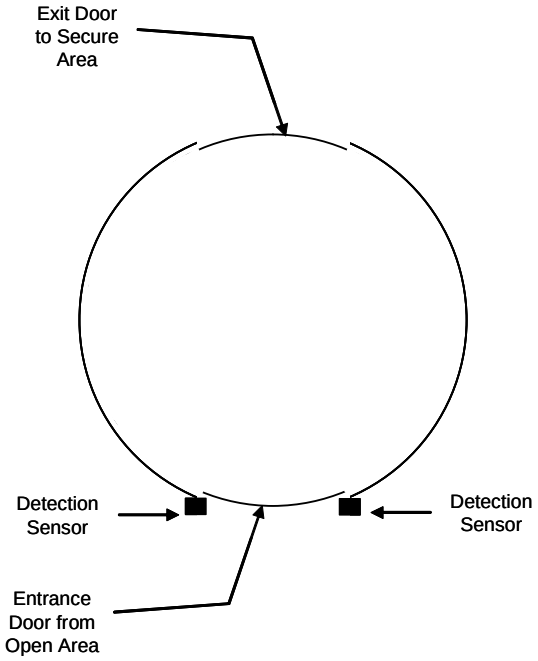

Figure 5-38. Notational diagram of an automated metal or weapon detection portal.

This unit can greatly reduce manpower normally used in a typical screening process, as it places the burden upon the users of divesting themselves of metal objects until they are able to pass through the unit. However, it will always be necessary to have security personnel available to hand scan a person who is unable to determine what is causing the detector to alarm. It is also recommended that there always be oversight personnel capable of protected overwatch in the area as a knowledgeable adversary may be able to defeat this type of unit. The footprint of this product can vary from about 4 ft to 8 ft in either a rectangular or circular format. These units can range in price from $90K to over $120K.

For additional information contact:

Mary Green
Security Systems and Technology Center
Dept. 6461
(505) 284-5424
mgreen@sandia.gov

5.15.3 Automated Explosives Detection

Trace and bulk explosives detection that collects and analyzes surface or air samples is discussed in detail in Section 5.2. Security personnel must be present to prevent a person from by-passing or spoofing the system.

Millimeter-wave technology uses millimeter-wave cameras to screen for anomalies on a person's body (Figure 5-39). These devices, which may be active or passive, must be located approximately 10 ft from a person and must be able to view the person for approximately 2 seconds, either while walking or standing. A person must be funneled through a fairly narrow corridor (~ 3 ft wide) so that no other person can come between the subject and the millimeter-wave unit(s). This process is completely automated up to this point as the software that receives the millimeter-wave unit's data will identify any anomalies detected and then alarm. A detected anomaly does not always indicate explosives, which prevents this procedure from being totally automated. If a person is not completely divested of non-clothing items before being examined by the millimeter-wave unit, an alarm will occur and a security person must respond.

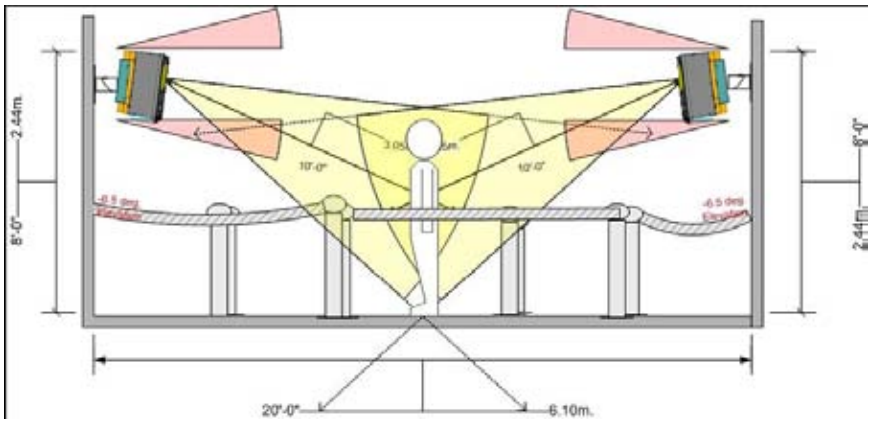

Figure 5-39. Millimeter-wave cameras examining a subject for anomalies.

The footprint of a millimeter-wave unit is fairly small—about 18 in. by 18 in. The space required for using these devices will be 10 ft for each direction—usually in front and in back of a person. Millimeter-wave camera systems cost between $50K and $80K each, with one unit required for each direction of view.

For additional information contact:

Eric Varley
Security Systems and Technology Center
Dept. 6418
(505) 844-0764
esvarle@sandia.gov

5.16 Perimeter Surveillance Radar System

Perimeter-monitoring, surveillance, and intrusion-alarm-and-tracking systems (see Figure 5-40 for examples) are commercially available, with production units in the field, and have been performance tested and compared. Tests were performed to determine baseline probability of sense[41] values at specified ranges under specified conditions and to quantify the effects of terrain and environmental factors (e.g., rain, high winds) on system performance. Limited data were gathered to characterize each system's NAR.[42] System characteristics, capabilities, and observed reliability issues were noted and documented for comparison purposes.

Figure 5-40. Examples of commercially available ground-based perimeter radar systems.

Ground-based radar (GBR) systems are designed for beyond-the-perimeter surveillance with the goal of providing early warning detection and tracking at low cost and low NAR. The systems scan areas with advertised sensing ranges of human-sized and vehicle-sized targets anywhere from 350 m (short-range GBR) to 10 km (long-range GBR) from the sensor unit. Radar sensors use reflected signals from targets to detect, locate, and track intrusions.

Both long- and short-range ground surveillance radar (GSR) systems require a line of sight from the radar antenna to the target and operate most effectively in open areas with minimal vegetation. A fence line located in a relatively flat, open area with minimal, low-growing vegetation and up to 1 km of open space on the inside of the fence line (depending on the radar system) is the most likely application for GSR systems. The radar system itself needs to have detection range-limiting settings and functions, or masking capabilities, in order to ignore alarms from movement in populated areas outside the fence.

[41]These tests were not conducted to determine probability of detection. They were designed and conducted to determine whether the sensor would sense the occurrence of an event within the sensor's field-of-view.
[42]Ideally, sufficient data would be collected and analyzed so that an estimate for the false alarm rate could be determined. This was not possible because of resource constraints imposed on the testing regimen.

Most GBR systems are provided with a graphical user interface (GUI) that can alert the operator during an intrusion, display and log the location and time of the intrusion, and allow the operator varying degrees of control and configuration of the GBR from the GUI. These systems have the capability to detect movement beyond the fence; however, the fence fabric can decrease sensitivity, especially at shallow angles to the fence line. Limited testing has shown that these radar systems will detect wildlife (large birds, rabbits, coyotes, etc.) and wind-induced movement of vegetation. In an area with significant wildlife activity, the NAR can be high. Heavy rain may also cause many nuisance alarms. On the display, alarms can appear as single or multiple hits (blips) that may or may not appear to have purposeful movement. The operator monitoring the display must therefore decide, with the aid of video assessment, which alarms are caused by nuisance sources and which are intrusion attempts.

Control of assessment cameras (i.e., infrared thermal and/or visible daylight) and camera positioning units has been integrated into some of the long-range radar systems. In those systems, the operator selects a target from the radar display for assessment. The radar system then provides coordinates and range information in a message packet sent to a pan/tilt zoom control unit. The camera then slews to the location of the target for assessment.

Costs range between $40K and $250K, depending on components, performance, and other system variables of system capabilities.

For additional information contact:

Frank Griffin
Security Systems and Technology Center
Dept. 642321
(505) 284-2599
fwgriff@sandia.gov

5.17 Counter-Sniper Remotely Operated Weapon System

One new tool that provides quick and effective response to sniper fire onto a nuclear site uses the ROWS, previously described in Section 5.4. The Counter-Sniper ROWS (CSR) integrates the data from midwave infrared detectors, which are capable of detecting a muzzle flash, with data from acoustic detectors, which are capable of detecting the crack or bang of a gunshot. The results of combining these data both detect the sniper fire and determine the location of origination. A network of ROWS platforms are then slewed to the target box location identified by the combined data from the acoustic and infrared detectors. An authorized operator then performs final aiming and weapon firing (Figures 5-41 through 5-45). An installation would require several infrared detectors, a number of acoustic detectors, several weapon platforms, and a control center. The actual installation depends upon site configuration and lines of sight.

Hardware costs for a basic installation with four infrared detectors, eight acoustic detectors, and four weapon platforms are estimated to be $2M. A more complicated site configuration will require more detectors and weapon platforms to achieve reasonable coverage. Infrastructure requirements include towers to raise the equipment to give line of sight to potential sniper loca-

tions, 120 VAC power to each equipment site, and fiber optic communications linking each equipment site. Installation, safety certification, testing, and training for a basic system will be $4M.

Figure 5-41. Counter-sniper infrared detector.

Figure 5-42. Counter-sniper acoustic detector.

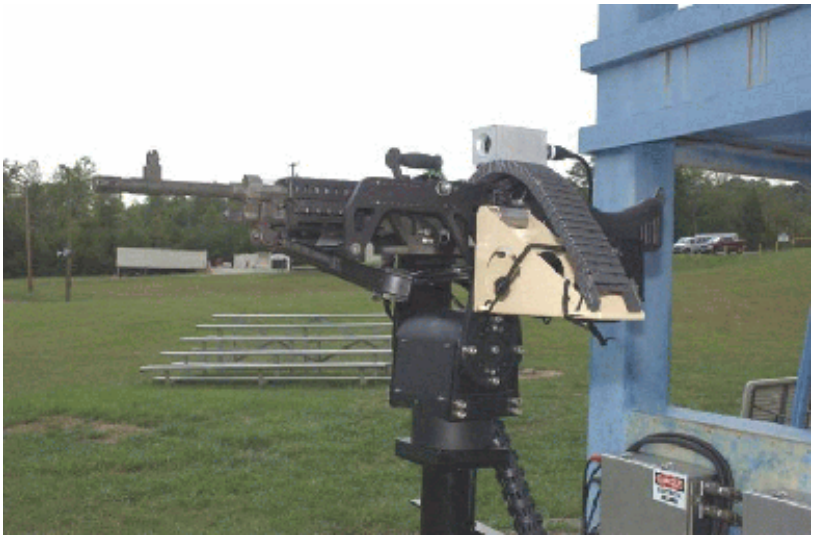

Figure 5-43. Example of a Remotely Operated Weapon System platform.

Figure 5-44. Counter-Sniper Remotely Operated Weapon System overview screen.

Figure 5-45. Counter-Sniper Remotely Operated Weapon System target screen.

For additional information contact:

Steven H. Scott, Manager
Active Response and Denial Dept.
Dept. 6422
(505) 845-8149
shscott@sandia.gov

5.18 Transparent Personnel-Shielding System

Developed at SNL for containment of a high-speed centrifuge, this unique security barrier can be installed quickly and economically for a wide variety of personnel-shielding applications. (See Figure 5-46 for an example application.) This containment system was tested with a 32-lb steel projectile traveling at approximately 60 MPH (88 ft/s). The polycarbonate thickness as tested is ½ in.; however, the design can accommodate a thickness range of ¼ in. to ¾ in. A bulletproof polycarbonate laminate, such as Lexgard®, could also be installed for protection against small arms fire.

Several commercially available products are combined in this unique shielding system that is far less expensive and quicker to build than the 4-ft-thick concrete walls or underground bunkers normally relied on for safety containment of heavy rotating machinery in the unlikely event of an accident. The first installed system at a DOE site was built in four days for about $30K, about one-tenth the cost of the proposed conventional containment structure of concrete and steel.

Figure 5-46. Patented polycarbonate/Unistrut® security barrier protects workers from flying debris.

The barrier system includes sheets of polycarbonate (clear plastic, such as Lexan®) glazed into frames made from Unistrut®, which are commercially available, pre-drilled steel bracings that fit together like pieces of a giant erector set. In industrial settings, Unistrut® is commonly used to create overhead tracks for electrical conduit, racks, shelving, stairs, and other structures. For machine containment, the impact-resistant transparent sheets provide the advantage of allowing operators to safely see the machinery behind the barrier during operation. For security applications, the transparent, modular, easy-to-install barriers can shield people from bomb blast shrapnel and terrorist small arms. It could be used in personnel portal applications and in bullet proof guard booths, among other uses. Sandia National Laboratories recently received a US patent on the modular barrier system for both machine-containment and security applications.

For additional information contact:

Keith Snyder,
Test Equipment Design Department
Dept. 2956,
(505) 844-6892
kwsnyder@sandia.gov

5.19 Silent Defender® Security Barrier

The Silent Defender® security barrier is an advanced security barrier in the configuration of a vestibule (see Figure 5-47). It has been designed by security experts to thwart attempts by well-equipped and well-trained adversaries attempting to enter critical and/or sensitive structures. Al-

though it functions as a normal door (see Figures 5-48 through 5-50), the Silent Defender® is a penetration-resistant modular passageway.[43]

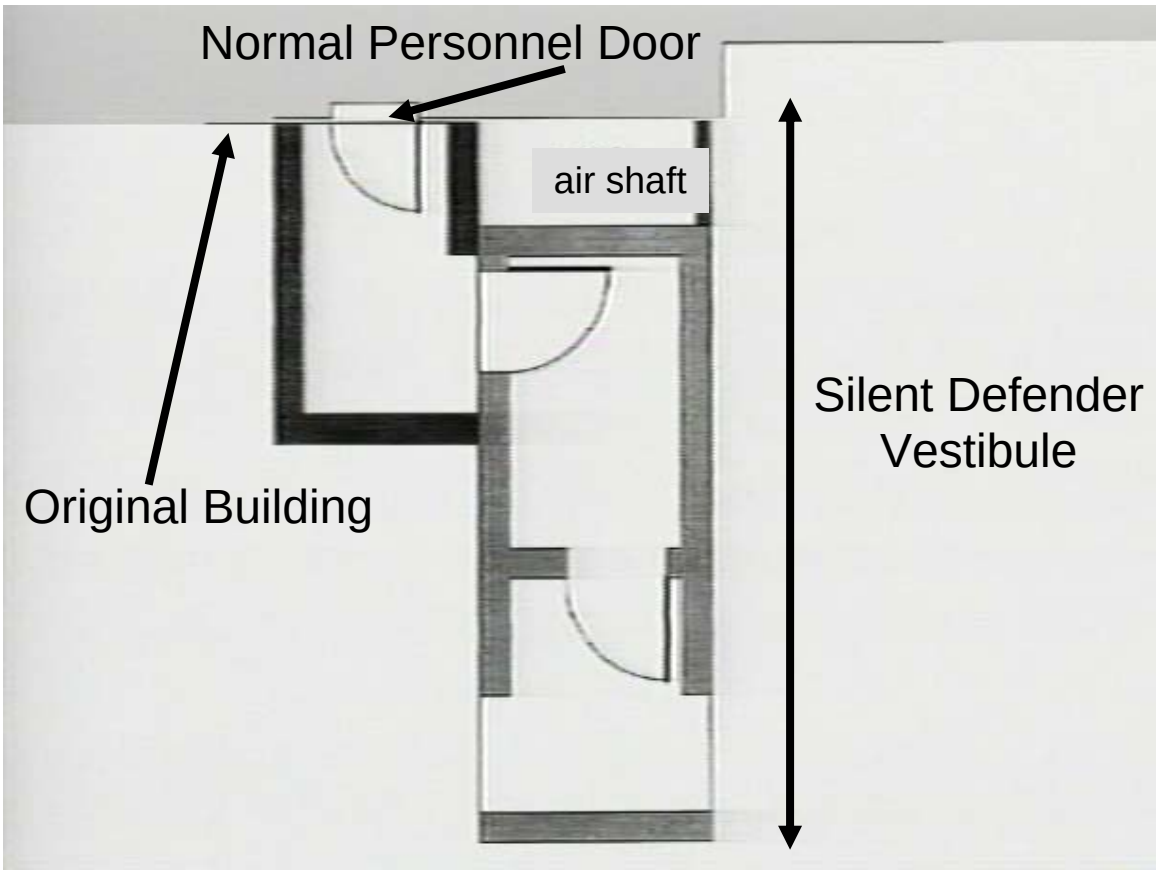

Figure 5-47. Top down cutaway view of Silent Defender® module attached to existing building.

Figure 5-48. Silent Defender® normal door function: approach.

Figure 5-49. Silent Defender® normal door function: opening.

Figure 5-50. Silent Defender® normal door function: closing.

[43]Figures for door function are from test structures. Actual doors would be enclosed by the vestibule.

The Silent Defender® is difficult and time-consuming to defeat, thus allowing sufficient time for security forces to assemble and respond to any attack, including the use of explosives. It is comprised of a concrete vestibule, a door frame, and a penetration-resistant security door that contains reactive delay features (see Figure 5-47). The vestibule is reinforced and follows SNL's barrier guidelines. It is attached to the customer's existing building as a foyer in front of the existing doorway (see Figure 5-47). The exterior security door is an armored steel front- and backface, reinforced with a steel grating (see Figure 5-51). Between the layers of grating are tubes filled with a foaming chemical agent. Also woven into the substructure is a cable system that flexes under extreme pressure (see Figure 5-52). The result is a barrier so formidable that even great amounts of explosives prove ineffective against it (see Figure 5-53). Unfortunately for an aggressor, the explosive charge fractures the internal tubes, instantly releasing a sticky foam that pools in front of the door, delaying any further aggressive action (see Figure 5-54).[44]

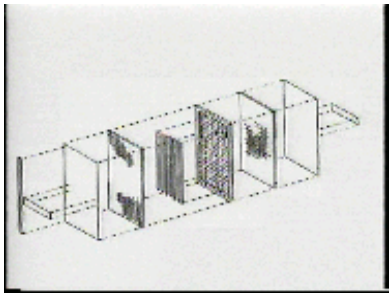

Figure 5-51. Silent Defender® door construction.

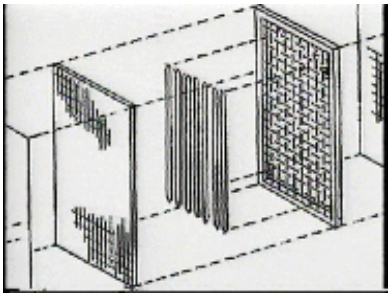

Figure 5-52. Silent Defender® door construction: details.

Figure 5-53. Silent Defender® being subjected to an explosion.

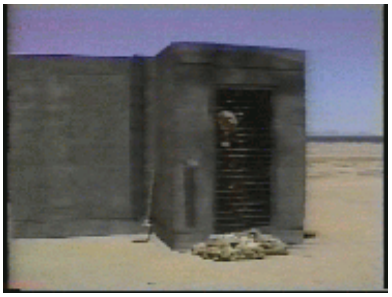

Figure 5-54. Silent Defender® with sticky foam pooled in front of door.

The Silent Defender® is manufactured by construction professionals who ensure that all aspects of the manufacturing are monitored with the strictest quality controls. Because it is a modular design, the Silent Defender® can be manufactured off site and delivered to the customer's location (see Figure 5-55) or constructed on site (see Figures 5-56 and 5-57). Off-site manufacturing minimizes the construction and security concerns that may affect the customer. Once the modules are complete, the Silent Defender® is attached to the existing structure in a relatively fast and simple process.

[44]Figure for the door is from a test structure. Actual doors would be enclosed by the vestibule.

Figure 5-55. Silent Defender® module delivered to site.

Figure 5-56. Silent Defender® module being constructed on site: door frame placement.

Figure 5-57. Silent Defender® module being constructed on site: concrete pour.

The Silent Defender® has been tested thoroughly with the assistance of the United States Air Force and Navy demolition specialists (see Figure 5-58). In test after test, with increasingly higher levels of explosives, the Silent Defender® remained a viable barrier. Moderate-sized holes that normally would have been adequate for intruders to pass through proved too difficult to penetrate due to the pool of foam and metal shrapnel on and around the door (see Figures 5-59 through 5-61).[45]

Figure 5-58. Silent Defender® testing team placing explosives.

Figure 5-59. Hole resulting from use of explosives on Silent Defender®.

[45]Figures for the doors are from test structures. Actual doors would be enclosed by the vestibule.

Figure 5-60. Shrapnel around hole in Silent Defender® door.

Figure 5-61. Sticky foam deployment from Silent Defender® door after explosion.

Silent Defender® protects resources, without the need for posting (additional) stationary guards at vital area entryways, thereby eliminating recurring personnel costs. Installing the Silent Defender® is a one-time expense. The Silent Defender® security barrier requires only routine maintenance and preventive maintenance. Calculations based on average costs indicate the Silent Defender's® payback period can be less than twelve months, depending on the application.

For additional information contact:

David Huttie
Director of Emergency Services Division
Arizona Public Service
(623) 393-3525
Albert.HuttieJr@aps.com)

6. OBSERVATIONS AND INSIGHTS FROM THE ORIGINAL DOCUMENT

The following section lists the **conclusions** from the original report and **comments** on the applicability of the original conclusion considering today's threat environment and the target audience to which this report is written (i.e., designers/builders of new commercial nuclear power plants). Finally, a concluding observation is provided that contrasts the focus of the original report with the focus of this report.

Conclusion 1: Structural design changes for pressurized water reactor plants (i.e., changes to building or plant arrangement) in and of themselves do not appear to provide significant additional protection against either the external or internal sabotage threat. Stated another way, all other things being equal, mere arrangement does not lead to significant changes in protection.

Comment: While this report does not address the details of current threat spectrum, most readers would agree that what *might* be considered in the current threat spectrum is somewhat different today than what was considered in the *expected* threat spectrum of the late 1970s and early 1980s. Thus, it is not necessarily surprising that the above conclusion was reached. However, with the current *potential* threat environment and this report's target audience, i.e., designers of new facilities, facility designers should consider building and plant arrangement when designing a facility.

Conclusion 2: Design changes can facilitate the implementation of more effective physical protection systems. For example:

- Design changes that restrict vital area access to a few well-defined routes, if appropriately combined with administrative controls and work rules, can increase the protection against the insider threat.

- Design changes that restrict outside access to a few routes (e.g., reduced number of outside doors), appropriately coupled with increased physical protection (stronger doors, more surveillance at selected locations, additional intrusion detection), will increase the protection against the external threat.

Comment: This conclusion should be as valid today as it was when first made, provided that the changes are part of a systems-integrated, well-balanced physical protection system–the goal of the design and evaluation methodology discussed in Chapter 2 of this document.

Conclusion 3: Damage control using installed systems in alternate (non-standard) ways has some potential for countering sabotage (or accidents). This damage control method requires additional study and probably some revision to current regulatory practice.

Comment: The scope (and purpose) of this revised document did not include the examination of a particular reactor design. As such, no definitive statement can be made as to the continued validity of the original conclusion. However, given the expertise of the authors (one of whom has more than twenty years experience in the various tasks associated with conducting probabilistic risk assessments for commercial nuclear power plants), the original conclusion might be found valid for new plant designs.

Conclusion 4: Damage control by running repair and/or jury rigging does not appear to be a viable counter to sabotage because of the associated operational impacts and the potential for an adversary to interfere with the damage control effort.

Comment: While the first part of this conclusion (i.e., the associated operational impacts) cannot be addressed by this report (because no specific facilities were examined), the last part (i.e., the potential for an adversary to interfere) would be as valid today as when it was originally made.

Additionally, the Nuclear Regulatory Commission has established six conditions necessary to be in place before credit for operator actions can be taken. If these conditions can be implemented, then operator actions can be credited.

Concluding Observation: The original report's focus was on light water reactor safety systems and re-configuration of them, layout considerations, and hardening of specific systems, structures, and components. This report's focus is on an iterative design and evaluation process that utilizes both facility design and physical protection system changes to optimize physical security. Nevertheless, much of the original report remains valid for many of the light water reactor designs being developed in the 2007 time frame.

7. SUMMARY

As indicated in Chapter 1, the U.S. Nuclear Regulatory Commission (NRC) has received several design certification applications recently, anticipates a few others, and has been notified of the intent of ten or more combined operating license applications between FY2007 and FY2008. To address this potential, the Commission directed the NRC staff to develop a draft proposed rulemaking that would require design certification and combined operating license applicants to submit security assessments with their applications. The proposed rulemaking was terminated, but the Commission directed the staff to complete the guidance so that applicants may utilize the information. The NRC tasked Sandia National Laboratories to revise the original NUREG/CR document. To ensure that the revision would be applicable (as a guidance document) in the current and future environment, the NRC staff directed that the revision employ a global rather than follow the design-specific approach of the original NUREG/CR. The global approach of the revised NUREG/CR is intended to be applicable to the many various designs being presented and to future Gen IV designs.

To this end the revised document provides high-level guidance for nuclear power plant design certification and combined operating license applicants as they:

1. develop the layout of a facility (i.e., how buildings are arranged on the site property and how they are arranged internally) to enhance protection against sabotage and facilitate use of physical security features,

2. design the PPS to be used at the facility, and

3. analyze the effectiveness of the PPS against the design basis threat.

This revised report does not provide specific recommendations for the design and evaluation of physical security for any specific reactor design. The guidance and best practices identified in this report are applicable to the design and evaluation of physical security for *any* plant.

An overview of the recommended approach for designing an effective PPS and analyzing its performance is provided in Chapter 2. This approach includes an integrated systems analysis to ensure that the physical protection elements function to minimize the likelihood that the PPS will fail to protect the targets it was designed to keep secure. A brief description of a representative set of currently available analytical tools that can be used in a security system performance assessment is provided in Chapter 3. A compilation of best practices that should be considered during the design of a physical security system is provided in Chapter 4. A brief description of a selected set of security system technologies that a nuclear power plant design team might consider during the design of the plant and its physical security system is provided in Chapter 5. As noted in Chapter 5, this list is representative of the technologies that are currently available or may become available in the near future (as of late 2006). Because this technology area is rapidly expanding, the designers of a new PPS should identify those technologies that are available at the time they design their PPS. Chapter 6 presents the observations and insights from the original NUREG/CR that are appropriate for this document (i.e., observations and insights that are general in nature and not design specific) and provides a comment as to the continued validity of the original observation/insight.

8. REFERENCES

1. Information Systems Laboratories, *Nuclear Power Plant Security Assessment Format and Content Guide*, Information Systems Laboratories, Rockville, MD, September 2007.

2. M. L. Garcia, *The Design and Evaluation of Physical Protection Systems*, Boston, Butterworth-Heinemann, 2001.

3. M. L. Garcia, *Vulnerability Assessment of Physical Protection Systems*, Boston, Butterworth-Heinemann, 2006.

4. G. B. Varnado and N. R. Ortiz, *Fault Tree Analysis for Vital Area Identification*, NUREG/CR-0809, SAND79-0946, Albuquerque, NM, U. S. Nuclear Regulatory Commission, Washington, DC, June 1979.

5. R. W. Youngblood and R. B. Worrell, *Top Event Prevention in Complex Systems*, American Society of Mechanical Engineers, Pressure Vessel and Piping Division (Publication) PVP, 1995, Vol. 296, p 153-159.

6. Sandia National Laboratories, *International Training Course 19*, SAND 2006-1987C, Sandia National Laboratories, Albuquerque, NM, May 2006.

7. D. Engi and C.P. Harlan, *Brief Adversary Threat Loss Estimator User's Guide*, SAND80-0952, Sandia National Laboratories, Albuquerque, NM, 1981.

8. D.M. Nicol and P. Heidelberger, *Parallel Algorithms for Simulating Continuous Time Markov Chains*, NASA CR-189729, 1992.

9. Analytic System and Software for Evaluating Safeguards and Security – User's Manual, Sandia National Laboratories, Albuquerque, NM, 1992.

10. JCATS Algorithm User's Guide, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-SM-213123.

11. SAVI: Systematic Analysis of Vulnerability to Intrusion Volume 1 of 2, Nuclear Security Systems Directorate and Science & Engineering Associates, Inc., SAND89-0926/1, Sandia National Laboratories, Albuquerque, NM, December 1989.

12. L. Kull, L. Harris, Jr., and J. Glancy, VISA—A Method for Evaluating the Performance of a Facility Safeguards System, in Proceedings of the Eighteenth Annual Institute of Nuclear Materials Management, Inc. Meeting, held in Washington, D.C., June 29 – July 1, 1977, in Institute of Nuclear Materials Management, vol. 6, no.3, pp.292-301, Fall 1977.

13. C. L. Nelson, 3-Dimensional Video Motion Detection and Assessment, SAND2004-0875C, Sandia National Laboratories, Albuquerque, NM, March 2004.

Distribution

1	MS0758	Learson, Berweida	6421
15	MS0759	Whitehead, Donnie	6461
1	MS0759	Biringer, Betty	6461
1	MS0762	O'Connor, Sharon	6421
1	MS0783	Potter, Claude	6422
1	MS0783	Scott, Steven	6422
1	MS1361	Varnado, Bruce	7654
1	MS9018	Central Technical Files	8944 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)