NUREG/CR-5899
SAND92-1339

# Entry/Exit Control Components for Physical Protection Systems

Prepared by
J. P. Holmes, B. T. Kenna, D. W. Murray

**Sandia National Laboratories**
Operated by
Sandia Corporation

**Prepared for**
**U.S. Nuclear Regulatory Commission**

## AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555

2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082

3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grant publications, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions. *Federal Register* notices, Federal and State legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

## DISCLAIMER NOTICE

NUREG/CR-5899
SAND92-1339

# Entry/Exit Control Components for Physical Protection Systems

Prepared by
J. P. Holmes, B. T. Kenna, D. W. Murray

**Sandia National Laboratories**
Operated by
Sandia Corporation

**Prepared for**
**U.S. Nuclear Regulatory Commission**

## AVAILABILITY NOTICE

### Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grant publications, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the Code of Federal Regulations, and Nuclear Regulatory Commission issuances.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions. Federal Register notices, Federal and State legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

## DISCLAIMER NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

NUREG/CR-5899
SAND92-1339

# Entry/Exit Control Components for Physical Protection Systems

Manuscript Completed: October 1992
Date Published: November 1992

Prepared by
J. P. Holmes, B. T. Kenna, D. W. Murray

Sandia National Laboratories
Albuquerque, NM 87185

**Prepared for**
**Division of Safeguards and Transportation**
**Office of Nuclear Material Safety and Safeguards**
**U.S. Nuclear Regulatory Commission**
**Washington, DC 20555**
**NRC FIN L1387**

# Abstract

The purpose of this NUREG is to provide technical information on the major components of entry control systems: identity verifiers, weapons detectors, explosives detectors, and special nuclear material (SNM) detectors. For each type of device, information is presented on principles of operation, hardware features, recommended installation, testing methods, and operational procedures. Applications to personnel, handcarried packages, bulk items, and vehicles are addressed.

# Contents

Page

# Figures



# Tables

# 1 Introduction

U. S. Nuclear Regulatory Commission (NRC) regulations under Part 73, "Physical Protection of Plants and Materials," of Title 10, Code of Federal Regulations, specify performance requirements for the physical protection of special nuclear materials and associated facilities.

For fuel cycle facilities using or possessing a formula quantity of strategic special nuclear material, section 73.45 (b) (2) (i) requires licensees to detect attempts to gain unauthorized access or introduce unauthorized materials into material access areas (MAAs) or vital areas (VAs) by deceit through access authorization controls or procedures. Furthermore, paragraph 73.45 (e) requires the removal of only authorized and confirmed forms of strategic special nuclear material from MAAs. Paragraph 73.45 (f) (2) (i) requires the provision for authorized access and ensurance of detection of and response to unauthorized penetrations of the protected area (PA) through access authorization and control procedures.

For these facilities, an example reference system is outlined in section 73.46. Specifically, paragraph 73.46 (d) requires an access control system to include a numbered picture badge identification system, written access control procedures, control of all points of personnel and vehicle access into the PA, and searches of individuals, vehicles, and handcarried packages for firearms, explosives, and incendiary devices. All points of personnel and vehicle access to MAAs must also be controlled. Individuals, vehicles, materials, and packages exiting from MAAs must be searched for concealed strategic special nuclear material.

Power reactor licensees are subject to the provisions of section 73.55. Specifically, paragraph 73.55 (d) requires th control of all points of personnel and vehicle access into PAs with identification and search of individuals and vehicles. The search function is for the detection of firearms, explosives, and incendiary devices. Packages and material for delivery to the PA are required to be searched similarly. A numbered picture badge is required for all individuals authorized unescorted access to the PA. Positive control is required of all points of personnel and vehicle access to VAs.

This document presents the views of Sandia National Laboratories on selected elements of entry/exit control in the physical protection of fixed sites. By virtue of the nature of a NUREG document, the discussion of equipment, procedures, or systems herein does not constitute acceptance or endorsement by the NRC.

# 2 Entry/Exit Control as Part of a Physical Protection System

## 2.1 The Role/Objective of Entry/Exit Control

The primary objective of controlling access to controlled areas is to ensure that only authorized persons with a legitimate need be allowed access to such areas. The objective of searching vehicles, personnel, and packages prior to entry into these areas is to prevent the introduction of contraband items that could be used to commit sabotage, or to aid in the theft of special nuclear material (SNM). The primary objective of exit control is to conduct searches of personnel, vehicles, and packages to ensure that concealed SNM is not removed. A secondary objective of entry/exit control is to provide a means of accountability for personnel during and after an emergency.

## 2.2 Components of Entry/Exit Control

### 2.2.1 Access Control

The components of access control include boundaries and other barriers to uncontrolled movement of all personnel into and out of sensitive areas. The operation of these components can be under manual control, automatic control, or a combination of both. A lock may require a key, a card, a combination, or a password to open. The requirement for the user to have a possession or knowledge to gain access is a valid element of access control. Identity verification may be accomplished either manually by using the guard force to identify a person, or automatically, such as by using a biometric verification technique. Card access control systems use coded cards to enter information into the card readers. A biometric identity verifier may be added as a series element between the card reader and the rest of the system. In operation, the verifier intercepts messages from the reader and requests the user to submit his/her biometric for verification. If the verification is successful, the card message is passed on to the entry control system. Otherwise, it is blocked. Fully automated entry control systems generally incorporate safeguards to prevent unauthorized access attempts. These safeguards may include tamper detection sensors, line security supervision, door monitor switches, authorization verification checking, personal identification number checking, personal identity verification, personnel tracking, and two-door portals.

#### 2.2.1.1 Identity Verification

Identity verification is the process of comparing an individual's features to a set of physical descriptors and making a decision as to whether or not they are from the same individual who originally enrolled in the system. The key component of identity verification is the authenticated set of physical descriptors unique to the individual being verified. The verification process can be performed manually or automatically. A common means of manual identity verification is the visual comparison of an individual's face to a photograph. Automatic identity verification can be performed by comparing a biological measurement (biometric) of an individual to a stored reference measurement obtained from a prior enrollment. Commercially available systems exist that perform automatic identity verification. Biological features that have been used for automatic identity verification include, but are not limited to, eye features, hand geometry, signature dynamics, typing dynamics, and voice dynamics.

#### 2.2.1.2 Coded Cards

A coded card contains machine-readable information and is used to rapidly read a person's claimed identity into an automated access control system. There are many coded card technologies that have been put into commercial use, including an optical code, bar code, magnetic spot, magnetic stripes, Wiegand-effect, proximity, capacitance, and integrated circuit or "smart" card technology. When a person presents a card at a reader, he/she is claiming to be the authorized holder of that card. The system then either authorizes the person to enter or rejects the entry.

#### 2.2.1.3 Authorization Verification

Authorization verification is the process of confirming that an individual is allowed entry or access to a particular resource or area of the facility at a particular time. This is done by checking the entry/access request with an authenticated authorization list. This verification process can be performed either manually or automatically. If performed automatically, the person could use a coded card that tells a computer his/her claimed identity, and the computer would search its controlled data base to automatically verify that the person is authorized to enter that certain area. This computer also is often used to keep a record of entry and exit, as well as to provide a real-time inventory of people for safety purposes.

#### 2.2.1.4 Entry Control Area Floor Plan

The efficient protection of controlled areas requires an integrated combination of entry control, guards, physical barriers, intrusion and tamper detection sensors, alarm annunciation, alarm assessment, and a response force. Entry control provides for authorized entry and exit of personnel, vehicles, and

packages into and out of the controlled area. Physical barriers are required to prevent the free movement of personnel, vehicles, and packages into and out of the controlled area. Intrusion sensors and patrolling guards detect unauthorized movement attempts and generate alarms to the site security control center. Alarm assessment, made by guards on the scene and/or at the site security control center from surveillance camera pictures, dictates the action of the response force.

The entry control area floor plan should provide for the efficient flow of traffic into and out of the controlled area. Specific areas should be provided for personnel identity verification, personnel authorization verification, personnel screening for contraband items, package screening for contraband, and holding areas for personnel and packages that do not pass the verification or screening tests for entry. Separate areas should be provided for entry and exit traffic where the traffic volume could be high enough to cause delays and/or confusion. Holding areas should be separated from the normal traffic flow to prevent delays to authorized traffic.

Physical separation and/or shielding should be provided between equipment that may cause, or be affected by, mutual interference. Remote badge readers, identity verifiers, computers, communication equipment, x-ray equipment, metal detectors, and explosives detectors are examples of equipment that may require such consideration. Manufacturers' specifications and FCC compliance certificates provide clues to potential problems. Manufacturers can usually provide additional information on proper installation of their equipment.

#### 2.2.1.5 Data Base Management

Data base management is the generation, maintenance, distribution, usage, and protection of entry control information. The sensitive nature of this information and the necessity to have authenticated data impose the need to protect much of this data from unauthorized access. Controls should be in place to protect sensitive data, in any format, from unauthorized access. This includes computer data files, video terminal screens, and hardcopy printouts/reports.

#### 2.2.1.6 Computers

Computers are routinely used for many tasks in entry control, from simple recordkeeping to complete automation of the entry control functions. A computer may be configured to stand alone, without a direct communications link to any other part of the entry control system, or, more often they are found in a network of communications links throughout modern entry control systems. Recent reports of widespread unauthorized access to government and bank computers serve to illustrate the vulnerability of this part of the access control system.

#### 2.2.1.7 Communications Systems

A modern entry control system can be spread over a wide area, with distributed processors controlling, monitoring, and reporting the various operations. Communications links between the system elements provide the paths for data transfer and allow for central monitoring and control of the entire system. Hard-wired communication links are generally preferred for fixed-site operations because they are easier to secure than radio frequency (RF) links. Line security is required for the protection of sensitive information and for ensuring the authenticity of received data. Data encryption, data authentication, and active line supervision techniques are methods to secure communications lines. Physical protection of the lines may provide sufficient security in some restricted areas. Redundant lines, following separate paths, protect against the loss of communication from a single incident.

### 2.2.2 Detection of Contraband Items and SNM

Contraband detection is for the purpose of preventing personnel from bringing into controlled areas items that can be used for sabotage and/or the unauthorized removal of special nuclear material (SNM) from facilities. SNM detection is for the express purpose of detecting the unauthorized removal of SNM from a material access area. Examples of contraband items are firearms, explosives, and incendiaries. Firearms are detected through the use of portal metal detectors for personnel screening and x-ray scanners for package search. Explosives are detected with the use of walk-through explosives detectors for personnel screening and handheld explosives detectors for package screening. SNM detection is achieved through the combined use of radiation detectors and metal detectors. The purpose of using both radiation detection and metal detection is that if the SNM is shielded in an attempt to defeat the radiation detector, the metallic shielding will be detected by the metal detector. Metal detectors and explosives detectors are useful for personnel screening while x-ray scanners are used for package screening. Alternate methods for performing personnel searches are the pat-down and strip search. Direct inspection of opened containers and packages is an alternate method for screening packages for contraband.

### 2.2.3 Intrusion Detection and Assessment

Intrusion detection sensors and tamper sensors for the entry control devices are incorporated into entry control systems to protect against unauthorized access. Sensors range from simple switches to sophisticated motion detectors. Alarms are generated when sensors detect an unannounced intrusion or a person attempting to enter the facility without going through the entry control portal. Alarm assessment is used to determine

the validity and the nature of the intrusion and can be used to determine appropriate response. If assessment cannot be made, worst case should be assumed by the response force. Direct assessment by the guard force has been the traditional method. Video camera assessment is being used in many systems because it provides for more rapid assessment, protects members of the guard force from possible open fire, and makes more efficient use of the guard force. Alarm and assessment data are usually sent to the site security control center. There may also be a separate location where the automated entry control system is monitored and controlled. Some or all alarm data may be sent to this entry control monitoring location in addition to the data sent to the site security control center.

## 2.3 Interface with Other Systems

### 2.3.1 Security Alarm Monitoring

Because a fault in the access control system or its defeat by an adversary could compromise site security, monitoring of critical access control function alarms may be required at the site security control center. It is the responsibility of the site security planner to determine which access control functions, if any, need such alarm monitoring. Failures of the access control system host computer(s) and unacknowledged access control alarms are access control faults that impact site security, and they are usually selected for monitoring by the site security control center.

#### 2.3.1.1 Computer Failures

Failures of the access control computers are monitored with the aid of a device referred to as a watchdog timer. A watchdog timer is a device that has an internal countdown clock that triggers an alarm relay when it reaches zero time. In use, the clock is electronically reset by the computer being monitored. The reset time interval is shorter than the countdown time interval, so the timer relay is not actuated as long as the computer continues to provide the clock reset signals. A failure of the computer stops the reset signals, allowing the clock to trigger the alarm relay. Actuation of this alarm relay should result in a security alarm.

#### 2.3.1.2 Access Control Alarms

Access control alarms should be acknowledged by an operator action within some time limit. Failure to acknowledge an access control alarm should result in a security alarm.

### 2.3.2 Guard Force Response Team

Duress alarms call for immediate responses. A failure by the primary site security control center to acknowledge access control alarms may also require that the secondary site security control center initiate an immediate response. A guard force response team may require direct notification of such alarms.

# 3 Personnel Entry/Exit Control

## 3.1 General Introduction

The elements of entry/exit control were briefly discussed in the first sections of this NUREG. The major sections of this chapter discuss the devices available for performing the functions of a personnel entry/exit control system: identity verifiers (3.2), weapons detectors (3.3), explosives detectors (3.4), and SNM detectors (3.5). Subsections for each component describe hardware, installation considerations, device testing, and operational methods. This chapter concludes with discussions of direct searches (3.6) and emergency evacuations (3.7).

## 3.2 Identity Verifiers

### 3.2.1 System Considerations

An identity verification system entails the consideration of a number of items concerning specific site considerations where the system is to be installed. Some of the items discussed below are applicable only to automated equipment. Many also apply to manual processes. Any site performing identity verification should establish criteria to ensure that the following items have been considered.

#### 3.2.1.1 Error Rates

The verification process requires the measurement of some biometric attribute. The measurement is analyzed and compared to a stored representation of the same biometric, which was obtained during user enrollment. If the match equals or exceeds the acceptance threshold value, the user's identity is verified and the user is accepted as who he/she claims to be. Otherwise, the user's identity is not verified and the user identity claim is rejected.

Two types of errors can occur in the identity verification process. A false rejection error is the failure to correctly verify the identity of a validly enrolled user. A false acceptance error is the incorrect verification of an imposter's identity as that of a validly enrolled user. The error rates are usually expressed as a percentage of occurrence and are functions of the acceptance threshold value. Figure 3-1 is typical of error rate behavior. As the false rejection error rates decrease, the false acceptance error rates increase. The choice of which threshold value to use is a trade off because there is no threshold setting where both error rates are zero. Low false acceptance error rates are associated with high security. Low false rejection error rates are associated with user friendliness. In high security applications, especially with few users, a relatively high false rejection error rate can be justified in order to provide a very low false acceptance probability. False rejection errors can cause unacceptable delays in high throughput applications, so a higher false acceptance probability may be justified in such applications.

#### 3.2.1.2 Verification Time

Verification time is the time span for the identity of an individual to be verified, from the time the process is started until verification is confirmed. The verification time affects the rate at which individuals can be allowed to pass through the Entry Control Station. Time becomes more important when there is a necessity for high throughput rates.

#### 3.2.1.3 Personal Identification Number (PIN) Management

Each authorized individual should be assigned at least one unique PIN, which will be an identifier for a particular record in the entry control data base. Additional PINs may be issued for the purpose of selecting alternate biometric information for backup verification, such as left hand in addition to right hand. Duress PINs may be issued to allow individuals to alert security to a problem without calling attention to themselves.

#### 3.2.1.4 Data Base Management

Individual records can be stored in one or more data bases for the purpose of controlling the entry/exit transactions. If more than one data base is used, a master data base should be designated. All changes to individual records should be made only at the master data base. All other data bases can be updated from the master, as conditions warrant, to keep the distributed data bases current. It is essential to protect the integrity of the data bases and prevent alterations by unauthorized individuals. A system may be implemented so that changes to the data base can be made only after the log on and identity verification of two authorized individuals.

#### 3.2.1.5 Individual Accounting and Backup

Individual accounting for the number and identity of individuals within the controlled areas can be accomplished when automatic identity verification is performed at both entry to and exit from each area. This accounting can be used to automatically detect any attempted violation of the two-man concept and passback, where more than one individual

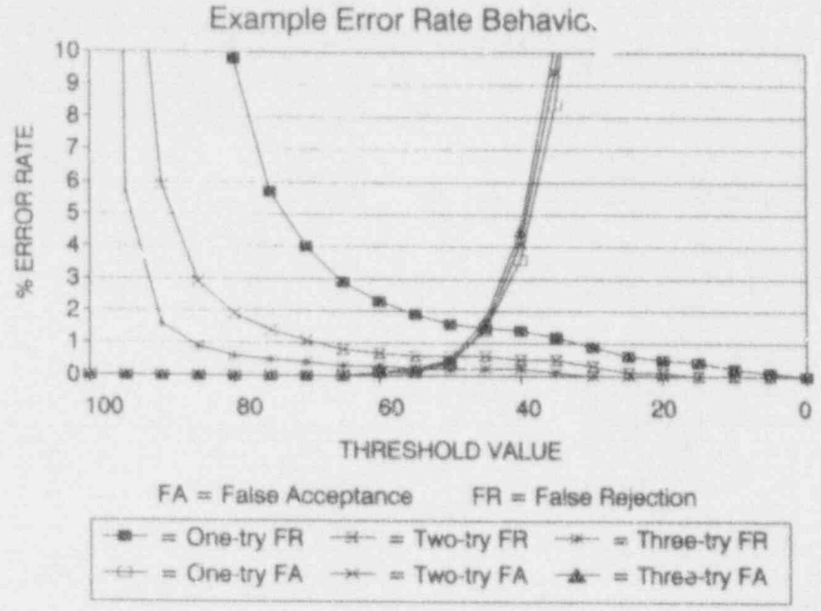



**Figure 3-1. Example error rate behavior**

attempts entry or exit with the same credentials. This accounting method can also be used to account for the last known location of individuals following an emergency. A record of all transactions can be generated and stored in a data file on the access control computer system. These records can be used to generate reports and audit trails of past transactions. A manual backup means of entry/exit should be provided at all times to accommodate authorized individuals who experience false rejection on automatic identity verification processes. Standby manpower for manual backup and standby system components for manual or automatic switchover should be available at all times.

#### 3.2.1.6 Emergencies

Provisions should be made for rapid entry/exit under emergency conditions. Evacuation routes and assembly points should be designated and training performed to minimize the confusion during an emergency situation. An automated entry control system can be used to account for personnel after an emergency, if entry and exit verification was in effect before the emergency and if follow-up verification is performed by all individuals at the assembly point(s) after the evacuation.

#### 3.2.1.7 System Security

The security of the identity verification system should be protected from compromise by unauthorized access. All components should be either inside secure areas or supervised to prevent compromise. The level of security protection should be consistent with the operation being performed. System access to enter or change security information may necessitate two authorized individuals to log on to the system and to undergo identity verification. Access to read-only files may necessitate only one authorized individual to log on and to undergo identity verification. Data encryption may be needed to prevent compromise for data routed through unsecured areas.

### 3.2.2 Hardware Description

#### 3.2.2.1 Coded Cards

Coded cards contain machine-readable information that can be used to rapidly read a person's claimed identity. Coded cards are in wide use throughout industry, and many different types of cards are commercially available. The following is a listing and description of some of the most popular cards. Many card features have been standardized under the American National Standards Institute (ANSI) and the International Standards Organization (ISO).

**Optical Card**

Two optical card technologies exist today. Optical memory, or laser, cards use compact disk technology to store several megabytes of data on a card. Optical spot cards use an array of optical transmission filters to modulate light into coded information.

Optical memory cards have a reflective surface that can be written on by burning spots into it with a laser light source. These spots can be detected by a low-intensity laser-optical system to read the written information. Special read/write hardware is required to accurately position the laser light on the card surface. Most of these cards use the "write once, read many" (WORM) technology. That is, the writing process permanently alters the surface so that it cannot be used again to store different information. These cards have the memory capacity to store several megabytes of information.

Optical spot cards contain rows of spots that show a different level of transparency when illuminated with a specific type of light. The card reader consists of an array of light sources and photodetectors. When the card is inserted between the light sources and photodetectors, the photodetectors read the relative transmissivity of the selected spots and translate them into the identification number. To make duplication of the card more difficult, the optical-coded card may contain several levels of transparency so that the optical transmissivity of the spots must fall within a specified range in order to be recognized as a valid code. Alternatively, the card may be printed with ink that is opaque to visible light but presents a different level of transparency to infrared light. Both techniques offer some protection against tampering and counterfeiting. Such a card is durable and low in cost. Up to 40 bytes of information may be encoded into the card, enough for a 12-digit number.

### Bar Code Card

A bar code is a group of parallel bars of different widths separated by light spaces. Variations in the widths of the bars and spaces between them are used to establish the code. To read the code, an optical bar code sensor scans the bar code and transmits the information to a decoding unit. Bar codes can be hidden from visual inspection by the use of special inks and cover materials that still allow the codes to be read by infrared wavelength scanners. Bar codes nominally contain 6 characters per inch, up to 12 characters.

### Magnetic-Spot Card

Several magnetic-spot card systems are presently in wide use. This card contains a barium ferrite inner layer on which an array of up to 40 spots has been permanently magnetized. The code is determined by the polarity of the magnetized spots. The card reader contains either magnetic sensors, which are electrically activated, or magnetic-reed switches that are mechanically actuated when a magnetic spot is nearby. The flux density of the magnetized spots is about 100 gauss, and a magnetic field strength of about 1,000 gauss is required to degrade the magnetic spots. Thus, accidental erasure of the magnetic code is not a significant problem. The magnetic code can be examined easily with a magnetic viewer. It is not difficult to duplicate the card.

### Magnetic-Stripe Card

Magnetic-stripe cards are widely used in commercial credit-card systems and in entry control systems. A stripe of magnetic material, located along one edge on the back of the card, is encoded with card data. Most vendors manufacture and encode the magnetic-stripe card in accordance with the current American National Standards Institute (ANSI) standards. These cards are read by moving the card past a magnetic read head. Two types of encoding tracks are specified in the ANSI standard for magnetic-stripe encoding. Track I, used by the International Air Traffic Association (IATA), allows up to 79 alphanumeric characters to be encoded. The use of the alphanumeric IATA coding allows the card holder's name to be included in addition to the card number. Track II, used by the American Bankers Association (ABA), allows up to 40 numeric characters to be encoded.

Three materials have been utilized as the magnetic-stripe medium. The most common material, a single-layer, 300-oersted magnetic stripe, has proven susceptible to accidental erasure. The second material, a dual-layer, 300/4,000-oersted tape, provides erasure protection on the 4,000-oersted layer. However, accidental erasure of the 300-oersted layer is still a problem. The third material, a single-layer, 4,000-oersted tape, is not susceptible to accidental erasure. It can also tolerate a greater separation between the tape and the magnetic read head, allowing a protective layer to be added to the magnetic read head. As a result, the 4,000-oersted tape can prolong the operating life of both the magnetic read head and the magnetic-stripe card. To read the card data reliably, the magnetic read head must be very near or in physical contact with the card. In case of physical contact, both the read head and the card are subjected to a moderate amount of wear and thus have limited operating lives. Operating the equipment in an outdoor environment can significantly reduce its lifetime. Field experience has shown that, in an outdoor environment, the magnetic read head can last 50,000 reads, compared with 250,000 reads indoors. The magnetic-stripe card is low in cost, moderate in the amount of information that can be encoded, and can even be encoded by the user. However, the standard card can be easily read and counterfeited with inexpensive equipment.

A new technique has recently been introduced that greatly increases the security of magnetic-stripe cards. It makes use of random jitter in the position of recorded signal features caused by several non-reproducible factors. These factors include timing variations of the motion while encoding, media irregularities, and the magnetic history of the medium. A

mathematical checksum calculation based on this jitter is used to detect any unauthorized changes to the data. Random prebiasing of the magnetic material and encrypting the checksum can be used to further enhance security. This technology requires licensing and the use of modified readers but is otherwise compatible with existing magnetic-stripe technology.

### Wiegand-Effect Card

The Wiegand-effect card contains a series of parallel Wiegand wires embedded in the bottom half of the card. The Wiegand wire is a specially treated ferromagnetic wire that produces a sudden, strong change in magnetic flux when exposed to a slowly changing magnetic field. Such strong magnetic flux reversals can be picked up easily by a sensing coil. Each Wiegand wire in the card is assigned a logic "0" or "1" by placing it in the proper position relative to the resetting magnets and the sensing coils. The Wiegand-effect card is impervious to accidental erasure. It is moderate both in cost and in the amount of information that can be encoded, about 40 bytes, or a 12-digit number. A magnetic viewer can read the card data easily, thus revealing the code therein.

### Proximity Card

The proximity card is one whose information can be read without the card being physically placed into a reader. Proximity cards can be classified in several ways. The three most common ways are (1) the method of powering the card, (2) the operating frequency range of the card, and (3) the read-only or read/write capability of the card.

The electronic proximity identification card, usually a small radio frequency transponder transmitter, must be powered in some way. Active cards are powered by a long-life battery packaged with the unit; the passive cards draw power from a transmitted radio frequency field as it enters the interrogation zone. Cards are classified into two groups according to frequency. Low-frequency cards range from 33 kHz to 500 kHz, while high-frequency cards range from 2.5 MHz to 10 GHz. The read-only card contains a specific code, usually fixed at the time of manufacture, which cannot be changed. The read/write card usually contains a larger data field than the read-only card and can be programmed by the system manager according to his/her needs. These cards are difficult to alter or duplicate. Several technologies are employed in producing the unique code on the card. The code length is limited to 12 or fewer digits for these proximity technologies. Three of these technologies are discussed below.

#### *Surface Acoustic Wave (SAW)*

In this type of code generation, RF energy is transmitted from the reader to the badge, then coupled to a lithium niobate crystal. This energy creates stress that produces a mechanical strain wave on the surface of the crystal. This wave is then coded by embedded metal transducers, which modify the wave as it travels across the surface. The coded wave is then detected and converted back to an RF signal, which is transmitted to the reader to be decoded.

#### *Integrated Circuit Card*

An integrated circuit card contains an electronic circuit that generates a digital code. This code is usually unique to each card. The electronics can be powered from either an external RF field or from an internal battery. Some cards are designed for fixed codes, which are inserted at the time of manufacture. Others allow for user coding. In operation, the card transmission is initiated by stimulation from the reader. The card responds by transmitting a signal that is modulated by the contained code. The reader receives and decodes this signal to identify the card.

#### *Electrically Tuned Circuits*

This code is produced by laminated, electrically tuned circuits that resonate at specific frequencies. The reader stimulates these cards by transmitting a wide band signal, which covers the range of frequencies of the tuned circuits. Each circuit responds to its specific stimulation frequency by absorbing energy and then re-radiating it at that frequency. The reader receives the re-radiated signals and determines the codes by detecting which frequencies are present.

### Capacitance Card

The capacitance card has an array of small capacitor plates laminated into it. Selected plates are connected to produce the desired code. The card reader measures the capacitance of the card to determine which plates are isolated and which are connected. The capacitance card is moderate both in cost and in the amount of information that can be encoded. The practical code length is limited to about 12 digits.

### Integrated Circuit Memory Card

Integrated circuit memory cards use solid-state, digital memory to store up to several megabytes of information. These memory-only cards can be written to and read from, almost without limit. These cards have limited application in access control because they are relatively easy to alter and duplicate. One type of integrated circuit, called a memory card, contains digital memory for storing information. These memory-only cards can store up to four megabytes of information.

#### Smart Card

Smart card technology, relatively new in the United States, has been in use for about a decade in France. The smart card, slightly thicker than a bank credit card, has a microprocessor and memory embedded in the card. The microprocessor gives the card its "smarts" and sets it apart from cards that only produce a single coded response. The size of memory on the smart card can range from a few kilobytes to over 100 kilobytes. The main advantage of the smart card is its potential for high resistance to forgery or compromise. Data encryption and biometrics templates can be incorporated to protect the card against unauthorized use. The primary disadvantage of the smart card is its relatively high cost.

### 3.2.2.2 Manual Identity Verification Hardware

Manual identity verification is based on the matching of physical features of an individual with an authenticated reference sample of the same features. Photographs, fingerprints, and signatures are common examples of techniques for manual identity verification. Hardware is commercially available that can capture, store, transmit, reproduce, and display reference samples of each of these examples.

#### Photographic Imaging

Facial imaging is the mainstay of manual identity verification for entry control. Security personnel can quickly match a person's facial image with a photographic image on a badge or a display monitor to verify identity. Photographic images may be obtained with either film or with video cameras. Film cameras generally have higher resolution capabilities than video cameras. Commercial hardware is available that will produce picture badges from either type of camera image. Video images are more suited to automated systems because they can be readily converted to digital format for transmission, display, and storage.

#### Fingerprint Imaging

Fingerprint identity verification has not been suitable for manual entry control until recently because direct observation of a fingerprint was not practical. Commercial hardware is now available that can capture and display a fingerprint image on a display monitor in near-real time. While this hardware has many advantages over the traditional fingerprint cards, it is relatively expensive. Fingerprint image comparison may have some applications in very vital areas, but it will likely require the use of specially trained operators and will likely be slower than facial image comparison.

#### Signature Imaging

Commercial hardware exists that can capture and display signature images for manual comparisons. While signatures have been a traditional method of manual identity verification, their value in entry control is limited. They have the same drawbacks as fingerprints and are more easily forged.

### 3.2.2.3 Automatic (Biometric) Identity Verification Hardware

Automatic identity verification is based on the matching of a measurement of a biological feature (biometric) of an individual with an authenticated reference measurement of the same feature. Automatic identity verification offers potential advantages over manual verification in both performance and cost.

Elements of performance for automatic identity verifiers are error rates and processing times for the various tasks being performed. Overall performance is a measure of how well a verifier meets the specific requirements of a particular application. Because requirements differ from one application to another, it is necessary to match the features of the verifier to the requirements of the application. The best verifier for one application may not be the best for another. Many commercially available systems exist which perform automatic identity verification based upon a variety of biometric features. These features and their associated sensors are discussed in the following paragraphs.

#### Eye Features

Two eye features that have been used for identity verification are retinal vascular patterns and iris patterns. Retinal patterns are used by commercially available systems. No system is yet available that makes use of iris patterns, although some efforts are being made to produce such a system.

The vascular features of the retina are sufficiently unique to an individual that a measure of these features can provide a very high confidence for identity verification. Measurements are made by optically sweeping a circular path on the retina with a low-intensity infrared light. The reflected light intensity is modulated by the presence of blood vessels, allowing the vessel positions to be located. Eye alignment, critical to successful measurements, is aided by a visual target in a viewing aperture, which guides the user to the proper position. In practice, this method has proven itself to be very reliable. Eyeglasses should be removed for scanning, but contact lenses are not a problem. People with very poor eyesight are more likely to be falsely rejected because of the requirement

to use a visual alignment target. False rejection has not proven to be a significant problem with this system, and a false acceptance is extremely unlikely. Figure 3-2 shows an eye feature identity verifier.

Iris feature extraction has been promoted as a non-invasive verification method. The iris has unique characteristics that can be used to verify an identity. Video imaging of the iris is the first step in feature extraction. The digitized image is usually normalized to minimize variations in scaling, rotation, and lighting before the features are extracted. Feature extraction has proven to be a problem in many cases where lighting and eye position are not carefully controlled. Glasses and contact lenses can produce reflections and shadows that complicate the feature extraction process. Dark eye features are more difficult to extract than those from lighter color eyes.

**Figure 3-2. Eye feature identity verifier**

### Fingerprint Features

Fingerprint features have long been recognized as unique to an individual. Several systems have been marketed to verify identity from some measure of a fingerprint. Various techniques have been tried to extract the unique features of fingerprints. Direct imaging, optical Fourier transform imaging, and linear scanning have all been successful. False rejection errors have been high in some cases of fingerprint identity verification. Imaging problems with the complex features of fingerprints can and do occur. False acceptance errors are extremely unlikely. Figure 3-3 shows a fingerprint identity verifier.

**Figure 3-3. Fingerprint identity verifier**

### Hand Geometry

The size and shape of the human hand have been shown to be unique to an individual. Commercial systems make use of thisfact to perform identity verification. One such system uses mechanical alignment pins to guide the hand into position for imaging. This helps to minimize processing complexity while producing very low false rejection and false acceptance error rates. This device is relatively fast and easy to use, making it a popular choice for entry control where a large number of users need to be verified. Another system, under development, does not require precise hand positioning. It uses software algorithms to correct for misalignment. Figure 3-4 shows a hand geometry identity verifier.

### Signature Dynamics

Signature verification has long been used to verify identity in the banking and finance communities. Signature dynamics verifiers record pen movements, while a user signs his/her name, to characterize features of the individual. A variety of methods have been employed for digitizing pen movements. Accelerometers, pressure transducers, proximity sensors, and acoustic sensors have all been used. The dynamic features of signatures are time dependent and prevent an imposter from simply tracing a valid signature to gain acceptance from the system. At least one system includes a signature

**Figure 3-4. Hand geometry identity verifier**

capture feature that allows for visual confirmation after the transaction. The error rates for false rejection and false acceptance are reasonably low for these systems, but tend to be higher than most of the physiological measurement devices. These devices also require somewhat more time to complete a transaction and are not as well suited for high throughput applications. They are very well suited for computer access control and for applications that traditionally require a signature, such as acknowledging receipt of sensitive items or information. Figure 3-5 shows a signature identity verifier.

### Typing Dynamics

Typing dynamics, or keyboard dynamics, verifies identity by the timing dynamics of entering a password into a computer keyboard. Even if an imposter knows the password, he will be rejected if it is not entered with the proper rhythm. The original products were implemented as a plug-in card that was inserted into the personal computer to be protected. The latest versions are implemented as a software product. Typing dynamics, which is suitable for computer access control, was not developed for personnel access control but may have applications in that area.

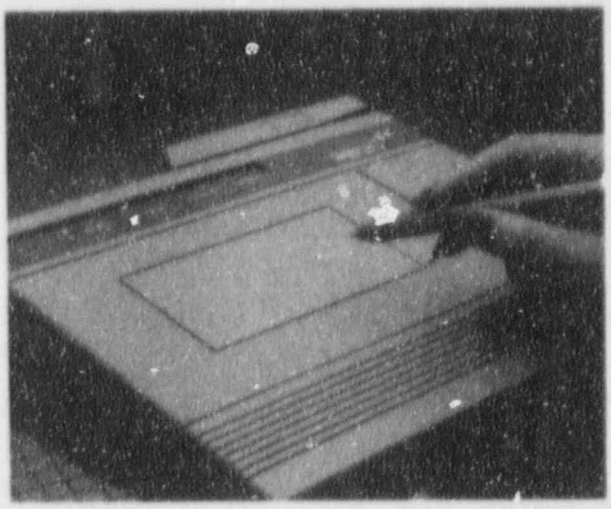


**Figure 3-5. Signature identity verifier**

### Voice Dynamics

Many companies manufacture voice dynamics-based identity verification systems. They range in complexity from small, simple phrase systems to elaborate systems requiring the user to repeat randomly generated number or phrase sequences. Random phrase requirements make it difficult to play back pre-recorded responses in an attempt to fool the device. There are also devices that are text-independent. They can identify or verify a speaker from voice samples, regardless of the text content. Transaction times are generally longer for voice systems than for other identity verifiers, especially for the ones requiring multiple responses. False rejection error rates can be affected by background noise. False acceptance error rates are generally lower for systems that require multiple voice responses. Voice dynamic verifiers are not well suited to high throughput access control applications.

## 3.2.3 Biometric Verifier Installation

Proper installation of entry/exit control hardware is paramount for correct operation of the equipment. Since there is such a wide variety of equipment, the persons responsible for detector installation should follow the manufacturer's recommendations. There are, however, some general guidelines that can enhance performance of the equipment. These general guidelines ensure proper installation of entry/exit control hardware.

Biometric identification devices are electronic in nature and usually have one or more of either mechanical, optical, or acoustic elements. They are all designed to operate in a protected environment, consistent with human habitation.

They are not suitable for outdoor use where moisture, dust, large temperature extremes, and other hostile factors may be present. Manufacturers can provide information on suitable operating environments for their equipment. Electromagnetic interference, noise, and lighting can affect these identifiers.

#### 3.2.3.1 Electromagnetic Interference

Electromagnetic interference is generally not a problem with these devices. They are comparable to a personal computer connected to a local area network. Strong electromagnetic field environments can cause problems, so they should not be placed adjacent to devices that generate these fields. Devices to be particularly wary of include x-ray machines, metal detectors, remote radio frequency badge readers, and switching power supplies.

#### 3.2.3.2 Acoustic Interference

Identity verifiers that utilize acoustic devices are susceptible to interference from background noise. Voice verifiers, for example, do not tolerate high levels of noise. One source of noise can be from mechanical vibrations transmitted through the mounting wall. Vibrations can be caused by equipment such as heaters, air conditioners, and electrically operated doors.

#### 3.2.3.3 Lighting Interference

Optical sensors can be influenced by background lighting conditions. Verifiers using such sensors should be protected from direct sunlight and other harsh lighting situations. A preferable arrangement would be to use a uniform lighting environment.

### 3.2.4 Biometric Verifier Testing

A biometric verifier's performance is best tested by subjecting it to controlled use by trained and impartial users and then analyzing the results. Training should be sufficient to bring the users to a point where they feel comfortable and confident with the verifier to be tested. Honest mistakes made by trained users are a normal part of the process in man-machine interactions and are a valid component in the test results. Partiality is a subtlety that can skew test results. The test population should not have a stake in the outcome of the test. The three values that most reflect verifier performance are false rejection error rate, false acceptance error rate, and transaction time.

#### 3.2.4.1 False Rejection Testing

A false rejection error is access denial due to the failure to verify the identity of a validly enrolled user. Testing to establish the false rejection error rate of a verifier is performed by recording the results of trained users making honest attempts at verification. The false rejection error rate is the percentage of verification failures that occur in a set of total attempts, with the allowable number of tries at verification and with the selected acceptance threshold value. Refinements and enhancements can be made on this simple approach to establish error rates at other acceptance thresholds and with a different number of tries allowed for verification.

#### 3.2.4.2 False Acceptance Testing

A false acceptance error is the incorrect matching of an imposter with a validly enrolled user and granting access. False acceptance testing requires trained users to enter the personal identification numbers (PIN) of other users and to attempt to be accepted as those individuals. The false acceptance error rate is the percentage of false acceptances that occur in the set of total attempts with the allowed number of tries at verification and with the selected acceptance threshold value. Refinements and enhancements can be made on this simple approach to establish error rates at other acceptance thresholds and with a different number of tries allowed for verification.

#### 3.2.4.3 Transaction Time Testing

Transaction time is the elapsed time for a validly enrolled user to gain access after initiating the identity verification process. An important consideration is that the transaction time of the verifier can be masked by other system delays when the verifier is connected to a distributed access control system; therefore, it is best to measure the verifier transaction time while the verifier is either in the stand-alone mode or while it is connected to a dedicated host computer with known delay times. Total system delay time is also significant in an integrated system. Testing of this time delay is discussed in the following section on qualification testing.

#### 3.2.4.4 Qualification Testing

Qualification testing of a verifier is best performed before it is put into service as part of an automated access control system. It is important to separate the verifier performance testing from the system debugging procedures. Any test results before the system is properly operating will be void. Error rates and transaction times can be established for the verifiers with a trained test population of about 10% the size of the expected user group. This will result in a representative sample of users if carefully chosen to prevent biased results. Each tester should perform at least 50 transactions to get past the learning inefficiency and become an effective user. System delays caused by high usage rates may be simulated by scheduling the entire test population to repeatedly verify as fast as the system allows.

Qualification testing performed after the system is put in service may include the entire population of a facility. This may be dictated by performance specifications or by the need to establish a baseline for future performance verification testing. Education and training of the entire test population are essential for the results to reflect true system performance. It may not be necessary, or even desirable, to inform the users that system testing is being performed. Monitoring of individual results is required in order to seek out individuals having unusual problems with the verifiers and to try to understand and to correct their problems. In some cases it may be necessary to exclude results from individuals who are unwilling or otherwise unable to properly use the verifiers.

#### 3.2.4.5 Verification Testing

Biometric identity verifier performance can be monitored automatically as the verifier is being used in daily operation. False rejection error rates and user scores are statistical variables whose distributions are a function of verifier performance. A running, long-term distribution of each of these variables can be generated as the verifier is being used. A short-term distribution of each of these variables can also be generated. A comparison of the long-term and short-term distributions will show differences that reflect changes in the verifier performance. Stable performance will produce similar distributions with nearly the same mean value. A significant change in verifier performance will cause the short-term distribution to deviate from the long-term distribution. A difference of the means of the two distributions can be used to trigger a performance alarm when a set threshold value has been reached. Initial threshold values for the differences can be set to three standard deviations of the long-term distribution. That is, if the difference of the means of the two distributions is greater than three times the standard deviation of the long-term distribution, an alarm is triggered. As experience is gained with the system performance, the threshold values can be adjusted to minimize false alarms and still be sensitive to performance changes. The length of time for the averages will be a function of the use rate of each verifier. A long-term average should have at least 1,000 transactions. A short-term average should have at least 30 transactions.

In more formal statistical testing, a standardized variable is used to detect significant changes:

$$z = \frac{\mu - \mu_0}{\frac{\sigma}{\sqrt{n}}}$$

where $\mu$ = short-term mean
$\mu_0$ = long-term mean
$\sigma$ = standard deviation of the long-term distribution
$n$ = number of samples in the short-term data set

The test for significant change assumes that no change has occurred. This is the null hypothesis, which assumes that $\mu = \mu_0$. This hypothesis is accepted if the absolute value of $z$ is less than some number, determined by a confidence value. Otherwise, the hypothesis is rejected, indicating that a significant change has occurred. These relationships are discussed in elementary statistics books that cover statistical testing.

### 3.2.5 Operational Methods

Having an effective entry/exit control system depends not only on having good equipment, properly installed and tested, but also on using the equipment correctly. The following paragraphs describe proven methods and other relevant considerations to ensure that the entry/exit equipment is used properly.

#### 3.2.5.1 Methods to Verify Identity

Identity verification can be performed manually or automatically. To facilitate both identification and search functions, entry and exit traffic should be separated by physical barriers, and employee and visitor traffic may be processed separately so that processing of visitors does not impede entry by employees.

**Manual Identity Verification**

One means for manual identity verification is facial recognition and positive comparison to an authorized picture badge. Positive comparison may be accomplished through a badge exchange or badge pick-up system. An alternate manual identity verification method is to use a facial image display monitor for recognition rather than a picture badge. This method uses an electronic photo-imaging system that captures, stores, and displays good quality facial images that are keyed to personal identification numbers (PIN). A facial image is displayed on a color monitor in response to the entry of its associated PIN. Facial recognition and a positive comparison to the monitor image provide the identity verification. PIN entry can be accomplished from a badge read as the person enters the entry/exit checkpoint.

**Automated Identity Verification**

A means for automated identity verification is by an identity verification device that uses a biological (biometric) measurement of the individual. Most biometric identification devices

need a protected environment such as controlled lighting and sound levels. Usually booths are built for such purposes, and procedures should be established to ensure that users move smoothly in and out of booths.

#### 3.2.5.2 Methods to Check Authorization

Authorization checking can be performed manually or automatically.

**Manual Authorization Checking**

One manual means of authorization checking is to confirm that the identified individual is on the authentic list of authorized individuals for entry at that location and time. It is the responsibility of facility security operations to generate, maintain, distribute, and protect the authenticity of the authorization lists. The authorization lists may be either hardcopy printouts or computer files that contain the required information and can be manually accessed.

**Automatic Authorization Checking**

An automatic means of authorization checking is to include the authorization data in the automated identity verification system so that it is automatically checked when identity is verified. This information would be included in the individual records in the personnel data base.

## 3.3 Weapons Detectors

### 3.3.1 Hardware Description

Weapons detectors are employed to detect firearms and incendiary devices. All firearms are constructed out of metal components. Even so-called "plastic" guns have metal barrels and springs, so the detection of firearms is the detection of metal. There are two general types of walk-through active metal detectors in use today, the most common being of the pulse type. The earliest active metal detectors, and still very viable, were of the continuous wave type. Regardless of the specific technology, all active metal detectors rely primarily on the fact that a time-varying magnetic field will induce currents in metal, and those induced currents can be detected. Metal detectors are widely used in security portals because of their speed of use, effectiveness at detecting firearms, and non-intrusive nature. The following paragraphs discuss the two types of walk-through metal detectors.

#### 3.3.1.1 Pulsed-Field Metal Detectors

The majority of metal detectors in use today for weapons detection employ a pulsed magnetic field. An electromagnetic pulse generated by the transmitter coil produces eddy currents in conductive metal objects within the archway which, in turn, generate their own magnetic field. The receiver coil or coils can detect this rapidly decaying magnetic field during the time between the transmitted pulses. (See Figure 3-6.) The magnitude and duration of the eddy currents and the associated magnetic field depend on the composition and geometry of the metal object.

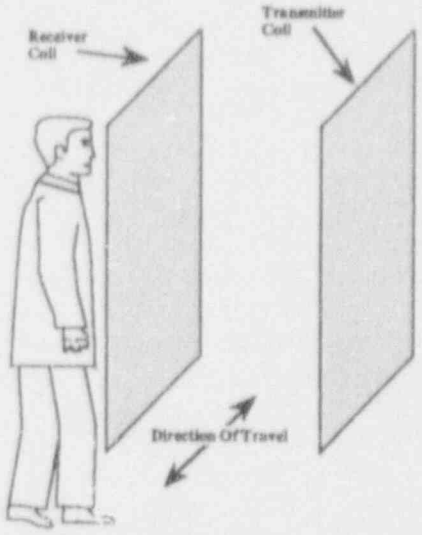



**Figure 3-6. Coil geometry for typical pulsed-field metal detector**

**Operation**

Metal detectors of the pulsed-field variety generate electromagnetic pulses in the range of 60 to 1500 pulses per second. The shapes of the pulses vary but generally have complex shapes: impulses, step functions, and square waves are common. The frequency spectrum of the waveforms contains frequency components from DC to 20 kHz. Coil configurations and signal processing vary from one manufacturer to the next, but the basic technology is the same. An electromagnetic pulse, on the order of 1 to 3 gauss, is transmitted by means of a coil built into the archway. After an interval following the transmitted pulse, the input from the receiver coil is sampled during a time window. The length of the interval after the transmitted pulse and the duration of the receive window depend on the operating mode and the specific type of metal to be detected.

**Eddy Currents**

When metal is subjected to a time-varying magnetic field, there is a voltage induced in any conductive path present in the metal. The induced voltage results in currents called Foucault, or eddy, currents. These currents in turn produce magnetic

fields of their own. The eddy currents induced in the target metal and their associated magnetic fields die out very quickly in small, highly resistive metal objects, while those in large, highly conductive objects persist somewhat longer. This is due to the fact that a larger voltage is induced in a larger object, and the induced current is greater in metals that are highly conductive. Another factor affecting the magnitude of the induced voltage is the ferromagnetic properties of the metal. Metals with a large relative magnetic permeability will have a larger induced voltage than an object of the same size that has a low relative magnetic permeability. Relative permeability is the permeability of the substance under consideration divided by the permeability of free space.

**Skin Depth**

Electric currents have a tendency to flow near the surface of the metal. This is called the skin effect. The depth that contains 63.2% of the current is called the skin depth. Skin depth is determined by the frequency of the current, the resistivity of the metal, and the relative permeability of the metal. For a given frequency, highly resistive nonmagnetic metals have a large skin depth while low resistive magnetic metals have a small skin depth. Metals with a small skin depth respond strongly to low frequency magnetic fields while metals with a large skin depth respond strongly only to higher frequency magnetic fields. When excited by the multi-frequency component magnetic field of a pulse metal detector, magnetic metals respond with eddy currents that are high in frequency. Nonmagnetic metals subjected to the same magnetic pulse will respond with high frequency eddy currents. This filter effect and other effects allow the more sophisticated pulse metal detectors to discriminate between the different types of metals.

### 3.3.1.2 Continuous Wave Metal Detectors

A second type of active metal detector generates a continuous, time-varying magnetic field within the archway. The signal is received by two receiver coils (see Figure 3-7), the outputs of which are fed to a balanced differential amplifier. As long as there is no metal in the archway, the balanced signal on each coil will result in no output signal. However, with the introduction of metal into the archway, the balance of the two received signals is disturbed, primarily due to eddy currents, and a signal will be generated. The processor can simply compare the signal to a threshold value to determine if an alarm condition exists, or it can compare the received signal to the transmitted signal to detect differences in the phase between the received signal and the transmitted signal. Detecting phase differences in terms of magnitude of the difference and the direction of the shift allows the detector to differentiate between different types of metals.

The most suitable frequency of the magnetic field for a given application is dependent upon the size and composition of the object to be detected. Low frequencies are useful for the detection of large ferromagnetic or large, high-conductivity, nonferromagnetic objects. For this reason, weapon detectors are usually low-frequency devices so that small metallic objects will not cause nuisance alarms. Typical frequencies for portal weapons detectors are around 300 Hz. Metal detectors designed to detect small metal objects employ frequencies up to 30 kHz. The higher frequencies required for smaller nonferromagnetic items are due to the fact that the excitation waveform is a sine wave. There are no frequency components (other than the fundamental frequency) to produce a significant response in the object. A non-sinusoidal wave or a frequency sweep would be required to produce the low- and high-pass filter effects present in pulse metal detectors.

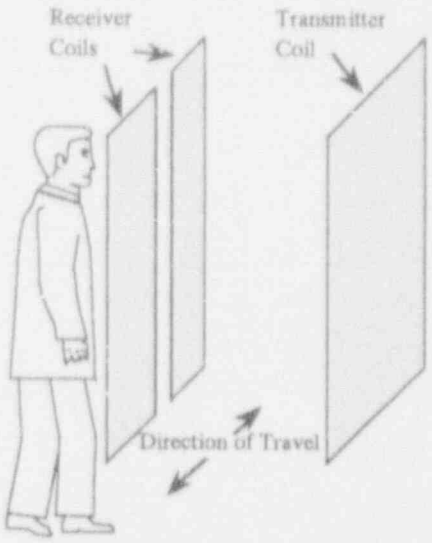



**Figure 3-7. Coil geometry for typical continuous wave metal detector**

**Absolute Mode vs. Differential Mode Screening**

When the responses to a group of individuals are recorded, the magnitude of most of the responses will be very close to the average response for the group. Further away from the average there will be fewer and fewer responses of that magnitude. When the number of responses at each specific magnitude is plotted against all possible magnitudes, a bell-shaped curve results. This bell-shaped distribution is referred to as a Gaussian distribution. In the normal mode of operation, continuous wave metal detectors are set up with a threshold that lies between the average response of the metal detector to a group

of people not carrying a threat item and the average response to the same group when carrying a threat item. (See Figure 3-8.) This mode of operation is called the absolute mode. This is fine for most weapons screening when the average responses are far enough apart so that for a high probability of detection there will be only a few nuisance alarms. However, when the threat item is small or hard to detect, the average responses are much closer together. (See Figure 3-9.) Now when the threshold is set to provide a high probability of detection, there will be a large number of nuisance alarms. Under these circumstances a different mode of operation may be more effective.

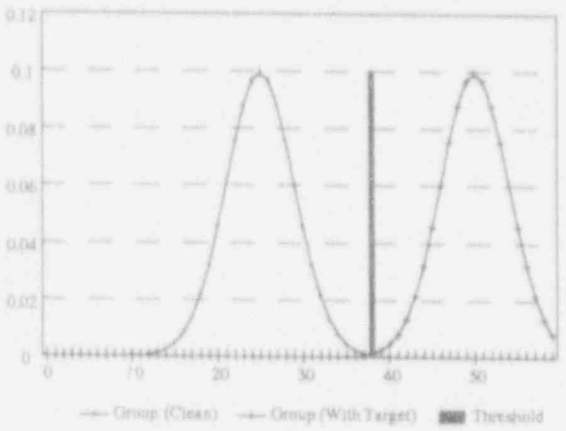



**Figure 3-8. Absolute mode screening for medium-to-large threat items**

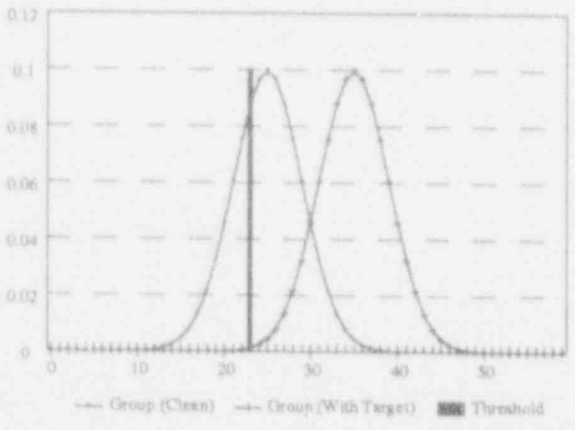



**Figure 3-9. Absolute mode screening for small and hard-to-detect threat items**

A differential (or relative) mode of operation takes advantage of the fact that the spread of the Gaussian curve (the variance) is typically much narrower for a single individual than for a group. Figure 3-10 shows that while the average response for an individual is the same as for the group, the distribution curves are considerably narrower. A threshold for that individual can now be established that maintains the probability of detection while significantly reducing the nuisance alarms. To operate in the differential mode, it is necessary to enroll each individual who is to be allowed into the area onto a data base. Each time an individual is screened, his/her response is compared against a threshold specific to that individual. The comparison can be made automatically by a detector or by a computer connected to the detector and the entry control hardware, or can be performed manually by security personnel.

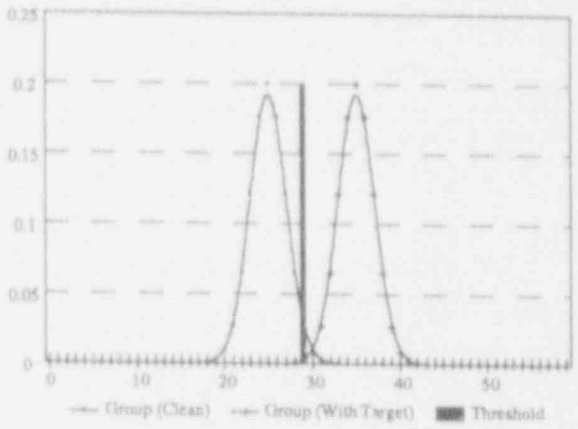



**Figure 3-10. Differential mode screening of small or hard-to-detect threat items**

#### 3.3.1.3 Detection vs Target Speed

Commercial metal detectors, both pulsed and continuous types, are optimized to detect metal moving through the archway at or near normal walking speed through the use of signal processing and filtering. The speed at which metal moving through the detector is detected is restricted so that static metal near the detector and electromagnetic noise caused by electric devices in the area will not cause nuisance alarms. Either technology may be used to design a detector capable of detecting small quantities of metal moving at a normal rate. The security officer supervising the metal detection should ensure that people being searched move at the proper speed. In most instances, metal detectors will have user-selected programs to vary sensitivity and speed response and to permit operation in a variety of modes.

### 3.3.2 Weapons Detector Installation

The primary consideration in the installation and use of weapons detectors is to reduce the nuisance alarm rate (NAR) to an acceptable value, yet keep adequate sensitivity. The nuisance alarm rate, as applied to metal detectors, usually refers to alarms caused by other metal objects, such as calculators, or alarms caused by an external event, such as lightning. These alarms will

be referred to as nuisance alarms to distinguish them from alarms caused by equipment failures or spurious noise internal to the metal detector. The latter alarms are commonly called "false" alarms.

#### 3.3.2.1 NAR Reduction Methods

Reduction of nuisance alarms in commercial metal detector equipment is accomplished in several ways. Electrical noise in the vicinity of the metal detector is a problem that is dealt with by filtering the AC power input and by processing spurious signals out of the received signal.

#### 3.3.2.2 Safety Shoes

Safety shoes can be a source of nuisance alarms at some facilities. Nonmetallic safety shoes are now available and may provide the best solution to this problem. An alternative would be to provide a change area so that safety shoes do not need to be worn through the metal detector.

#### 3.3.2.3 Static Metal

Most metal detectors have the ability to ignore static metal. This feature permits them to be positioned near stationary metal objects without going into constant alarm. However, nearby metal structures can still affect the sensitivity of a metal detector, and whenever possible a metal detector should be located at least three to four feet away from metal structures. Ferromagnetic structures, or materials with a relative permeability much greater than 1, can distort the transmitted field, disrupting the uniformity of the detection field. Nonferromagnetic metal structures can act as shields reducing field strengths. Metal in the floor should also be considered when installing a metal detector system. An elevated ramp or aluminum shield may be necessary to offset the effect of metal structures in the floor. Static metal can also provide a path to electromagnetic noise. Care should be taken to use proper grounding and isolation techniques to prevent a metal structure from conducting noise from a far-away source to the metal detector.

#### 3.3.2.4 Installing Near Other Equipment

Installing multiple metal detectors in close proximity or operating a metal detector in conjunction with x-ray equipment may require special installation procedures. When metal detectors operate at distances of less than 20 ft. apart, all detectors should be the same make and model. Consultation with the equipment manufacturers before installation can provide techniques to minimize the effects of interference from these sources.

#### 3.3.2.5 Interaction with Floor

Similar to the case of walk-through detectors, metal in the floor can be a problem with the handheld metal detectors. The handheld detectors, with their high sensitivity, can alarm when passed close to a floor that contains reinforcing bars. If the interference is minimal, a simple solution is to make sure that the paddle or loop of the detector is held vertical because the edge of the detection coil is the least sensitive. Holding the coil vertical will minimize the response to metal in the floor. If interference is still a problem, a wooden platform may be constructed on which the person being searched can stand. The construction method of the platform should make use of glue and other nonmetallic fasteners to prevent false alarms due to nails or screws.

#### 3.3.2.6 High-Sensitivity Operation Installation

Searching for very small metal objects or SNM shielding material imposes restrictions/limitations that are not necessary for weapons screening. Since the sensitivity of the metal detector is much higher than is needed for weapons detection, more attention should be given to sources of nuisance alarms. These include moving metal, such as a metal door in the vicinity of the detector, faulty lighting fixtures, building vibration, electric motors or transformers, radio frequency sources, or nearby wiring.

##### Site Selection

The site of a high-sensitivity metal detector should be selected carefully, and the power source for the metal detector should be relatively free from noise or power surges. Environmental factors that should be considered for every metal detector installation become even more important when greater sensitivity is required. The presence of steel or other metal in the floor, walls, or ceiling of a potential site should not be overlooked. A high-sensitivity metal detector should be located away from all metal objects.

##### Change Area

To prevent alarms on a high-sensitivity metal detector from clothing and jewelry, a change area and lockers may need to be provided. Metal components of shoes such as steel arch shanks can also be a source of alarms.

#### 3.3.2.7 Metal Detectors as a Source of Interference

While consideration is usually given to the effect of nearby equipment on a metal detector, occasionally a problem arises

because the metal detector itself can be a source of electromagnetic interference (EMI). Equipment likely to be affected would be telephone or video equipment placed near the detector's archway. The simplest solution is to move the equipment away from the metal detector, but if that is impossible, EMI shielding can be used. The disadvantage to using EMI shielding is that it is metallic and could alter the sensitivity of the metal detector. It is preferable to shield the equipment that is being affected rather than the metal detector.

## 3.3.3 Weapons Detector Testing

### 3.3.3.1 Test Object Considerations

Eddy currents and their associated magnetic fields are the evidence that metal detectors use to detect the presence of a conductive material. There are several test object-related factors that affect the magnitude of the eddy currents and therefore the magnitude of the metal detector's response. These major factors are the geometry of the target and its electrical and ferromagnetic properties.

#### Target Size

The geometry of the target influences the magnitude of the eddy currents in several ways. First, the cross-sectional area normal to the magnetic field is proportional to the induced voltage within the target. (See Figure 3-11.) Therefore, objects that have the same cross-sectional area have nearly the same induced voltage. If metal detectors simply responded to the induced voltage, objects with the same induced voltage would produce the same response. However, metal detectors respond to the eddy currents that result from the induced voltages. In accordance with Ohm's Law, the resulting current is proportional to the voltage and inversely proportional to the resistance. (See Figure 3-12.)

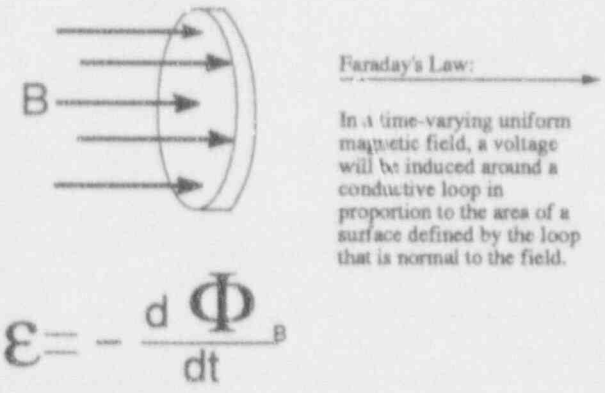



**Figure 3-11. Induced voltage**

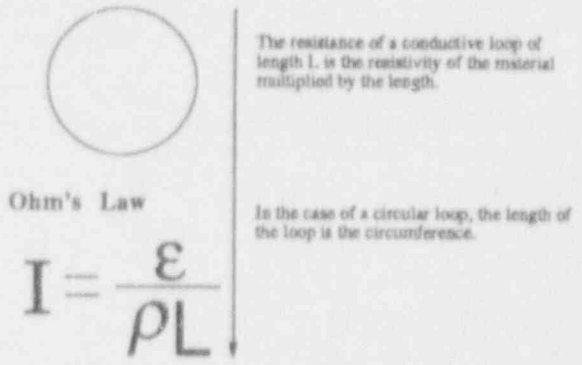
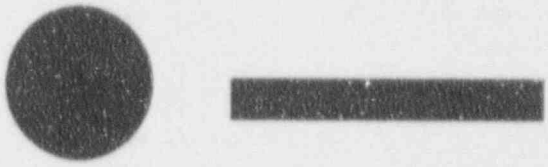



**Figure 3-12. Magnitude of eddy currents**

#### Target Shape

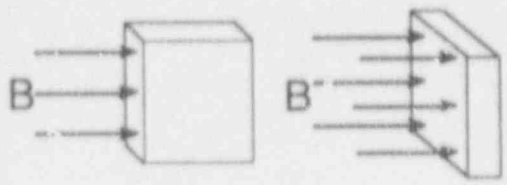
The shape of the target will be a major factor in determining the magnitude of the resistance of the conductive path of the target and therefore the magnitude of the eddy current. A given material has a fixed resistivity so the resistance of a target's conductive path is the resistivity of its material multiplied by the length of the conductive path. The length of the electrical path is effectively the length of the perimeter of a cross-sectional area of the target that intersects a plane normal to the magnetic field. An example is the case of a circle and a rectangle, both with an area of nine square inches. (See Figure 3-13.) If the rectangle has a length of nine inches and a width of one inch, the rectangle's perimeter is about twice as long as the circle's. Even though the induced voltage of each target is the same (because of equal area and Faraday's Law), the resistance of the rectangle is more than twice that of the circle.



Two shapes of the same material have equal areas. The 9-sq.-in. circle has a circumference of 10.53 in.; the 9-sq.-in. (9x1 in.) rectangle has a perimeter of 20 in. The resistance of the rectangular path is almost twice as high as the circular path. The result is that the circle is easier to detect.

**Figure 3-13. Shape**

The result is that the circle will produce an eddy current that is over twice that of the rectangle. Targets of complex shape will tend to produce smaller responses in a metal detector. Complex asymmetrical shapes also cause variation in response due to orientation by presenting different cross-sectional areas to the magnetic field. (See Figure 3-14.)




The orientation of an object can change the cross-sectional area that is normal to the magnetic lines of flux.

**Figure 3-14. Orientation**

### Metal Thickness

Skin depth refers to the fact that a current will be induced near the surface of a conductive material. This means that the thickness of the target (or the walls of the target) affect the magnitude of the induced voltage and therefore the magnitude of the eddy current. A target that is less than three skin depths in thickness will produce a lower response in a metal detector than one that has a thickness greater than three skin depths. In all the equations that describe the magnitude and duration of eddy currents in a target, only geometrical, electrical, and magnetic considerations enter into the calculations.

### Worst-Case Threat Item

The first step toward developing set-up and performance verification procedures is to identify a worst-case threat item that should always be detected. This task is made more difficult because the worst-case target is not necessarily the smallest target but rather the most difficult to detect. For example, a large brass object may be harder to detect than a small steel object. A handgun made of carbon steel is easier to detect than the same weapon made of a more resistive stainless steel.

## 3.3.3.2 Test Objects and Standards

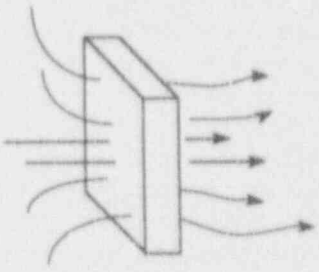
Several older standards for testing metal detectors described test objects in terms of mass and whether or not the metal contained iron (ferrous vs nonferrous). Older standards specified some masses of metals to serve as test objects. There was no attempt to define the objects in terms of specific metals or the geometry of the items. From the previous discussion, it should be obvious that two items of the same material and mass, but with very different shapes, can elicit greatly different responses in a metal detector. The following paragraphs discuss the importance of more specific standards for test objects.

### The Importance of Resistivity

The resistivities of the materials need to be specified. This becomes obvious when one considers the case of the nonferrous target. If copper is chosen as the nonferrous material for the test object, a target that will be easily detected will result. However, if the target is made of lead, the result will be a target that will be very difficult to detect. This is due to two reasons. First, lead is much more resistive than copper (about 14 times more resistive). And second, the lead target will be much smaller than the copper target because of the high specific gravity of lead. There are other metals that are much more resistive than lead. Clearly, the choice of the metal can produce responses that vary between saturation of the detector and not being detected at all.

### Ferrous vs Ferromagnetic

How one interprets this old standard requirement also depends upon the definition of ferrous. Strictly speaking, the word *ferrous* means being composed chiefly of iron. This is a chemical definition and not the electromagnetic definition that was probably intended. The standard should have used the word *ferromagnetic*. Ferromagnetic means that the material is attracted by a magnet. More specifically, a ferromagnetic material has a relative permeability that is much greater than one. The ferromagnetic properties of a material very much affect the response of a metal detector, while the ferrous properties of the material have no effect on the response at all. An example of this is the ferrous material stainless steel and the nonferrous ALNICO alloy, an alloy of aluminum, nickel, and cobalt. Austenitic, or non-magnetic, alloys of stainless steel are slightly paramagnetic while the ALNICO is highly ferromagnetic. A metal detector will respond to the stainless steel in much the same way that it does to a resistive nonferromagnetic metal, while the ALNICO will produce a response similar to the response to cast iron. See Figure 3-15.



By providing a path of lower reluctance than the surrounding medium, ferromagnetic materials distort the magnetic field.

By intensifying the magnetic field within their volume, ferromagnetic materials have a higher induced voltage than other materials.

**Figure 3-15. Ferromagnetic materials**

**Current Weapons Test Objects**

The choice of test object depends upon the function of the metal detector. Metal detectors used for entry control should use the weapons test objects described below. Those used for exit control should use the SNM shielding test object also described below.

(1) Steel and aluminum alloy .25 caliber automatic pistol. Manufactured by Armi Tanfoglio Giuseppe in Italy. Sold in the USA by Excam as model GT27B, and by F.I.E. as the Titan.

(2) Aluminum Model 7, .380 caliber derringer. Manufactured by American Derringer Corporation.

**Current SNM-Shielding Test Object**

The recommended test object for exit shielding for highly enriched uranium is a hollow lead cylinder with a diameter and length of 1 $^1/_4$ inches and a wall thickness of $^1/_8$ inch. However, where credible theft scenarios do not require the detection of an object this small or of this material, and where requirements are properly documented and approved, test objects suitable to a specific situation may be substituted.

### 3.3.3.3 Programmability and Test Objects

Modern metal detectors have become very flexible. The introduction of digital technology has led to an increase in programmability. By altering a program setting, one can change the way in which a metal detector will respond to the various metals. A metal detector can be adjusted to detect nonferromagnetic metals while nearly ignoring ferromagnetic metals. Altering the program can then reverse the situation where the nonferromagnetic metals are ignored. This ability to target specific metal types is a powerful tool but greatly complicates the task of testing and setting up the metal detector for weapons screening. Modern weapons are composed of a wide variety of metals and other materials, and they can be divided into three general categories: (1) those composed mainly of ferromagnetic materials, (2) those composed mainly of nonferromagnetic materials, and (3) those composed of both types of metals in roughly equal proportions. To ensure that the detector detects all of the three general types of handguns, the detector should be tested against a worst-case representative of each of the three groups.

A few decades ago, when nearly all guns were made of steel, the concept of an exemplar (or model) made sense. At that time all guns shared common characteristics. An exemplar could be devised that represented all handguns reasonably well. This is no longer the case. An exemplar made from ferromagnetic metal will, in this age of alloys, represent only a small percentage of handguns. On the other hand, an exemplar made from only nonferromagnetic metal would again represent only a small percentage of weapons that are composed of only nonferromagnetic metal. An exemplar that is composed of both ferromagnetic and nonferromagnetic metals would represent the majority of handguns on today's market but would still leave two types of weapons out of the test standard. A metal detector adjusted to detect a single type of gun will generally be vulnerable to other types of guns. Tests have shown that out of a group of five guns that are among the hardest to detect of all handguns, no single gun was the most difficult to detect in all detector/program combinations. If it is desirable to use nonweapons standards for metal detector testing and adjustment, a set of three exemplars representative of the three general classes of handguns (mentioned in the preceding paragraph) would be advisable.

### 3.3.3.4 Setup For Testing

**Clean Testers and Variability**

The set-up procedure for metal detectors usually involves a "clean tester" carrying target objects used to check the sensitivity of the detector. A clean tester is defined as a person carrying no significant metal. A troublesome variable in walk-through metal detector systems is that different people affect metal detectors differently. One person may carry a quantity of metal through a detector without causing an alarm while another person with exactly the same quantity of metal will cause an alarm. Some factors that contribute to this variability are walking speed, gait, and body composition. This effect becomes a consideration when setting up a metal detector as a weapons detector. A threshold should be set low enough to detect all weapons, but high enough so that the nuisance alarm rate does not slow traffic. When performing the initial detector setup, testing with a number of clean testers with differing body types will increase confidence that the detector will detect the threat objects when carried by anyone of any body type.

**Controls**

Controls commonly found on metal detectors are a sensitivity control and a program selection control. For most metal detectors, the sensitivity control is used to set the variable gain of receiver amplifiers while the threshold remains constant and generally has no effect on the transmitter. Some metal detectors adjust sensitivity by adjusting the alarm threshold while holding the receiver amplifier gain constant. The program control changes such variables as the transmitter frequency, filtering, and signal processing. Some detectors have

such flexible programming that they can be adjusted to detect either ferromagnetic or nonferromagnetic metal almost to the exclusion of the other. Other controls that may be present provide for the adjustment of the audible alarm's tone and volume; they also allow tamper acknowledge and access to diagnostics functions.

#### 3.3.3.5 Laboratory Characterization Testing

Attempts to determine probabilities of detection and nuisance alarm rates for metal detectors in a laboratory environment have met with limited success. Difficulties arise from the variety of metal detector configurations available and from the number of variables that affect their operation. However, there are a number of tests that can be performed that help to reveal many of the performance characteristics of portal metal detectors.

**Test Area Concerns**

When testing metal detectors for the purpose of making comparisons or evaluations, attention should be given to the test environment and to the test repeatability. The test environment should be free of metal and wide temperature fluctuations. Variables introduced by a "clean tester" can be reduced by using a non-metallic, mechanical device to move test objects through the metal detector archway. Devices built for this purpose usually consist of a wooden or plastic track over which an object can be pulled by means of a motor or handcrank. The purpose of using such a device is to eliminate the body effect and to precisely control the speed and placement of the test object. If a clean tester is used, the same one should be used for all tests. A mechanical tester should not be used, however, to perform the initial sensitivity adjustment during installation. Because of the body effect, the sensitivity setting required to detect a target carried by a person will generally be higher than to detect the same target transported by a mechanical tester.

**Uniformity of the Detection Field**

A metal detector is the combination of transmitting and receiving systems. The transmitting and receiving antennas are usually on opposite sides of the walkway. The transmitter generates an electromagnetic field in a pattern determined by the configuration of the transmitting coil or antenna. This field varies in strength as the inverse square of the distance from the antenna. Since the field strength falls off as the distance from the transmitter increases, the magnitude of the induced eddy current also falls off as the distance from the transmitter increases, suggesting that the area of lowest sensitivity would be on the receiver side of the detector. However, as the target is passed through on the receiver side of the detector, its close proximity to the receiver allows its smaller signal to be detected more easily. The result of these two competing effects, which has been confirmed during laboratory testing, is that the actual area of lowest sensitivity is near the middle of the detector archway. Another field factor that affects uniformity is the fringing of the magnetic lines of flux at the extremes of the transmitter coil. The fringing of the lines of flux causes areas of lower sensitivity at the top and bottom of the detector.

**Sensitivity vs Magnetic Field Strength**

The interaction of the two antenna systems primarily determines the uniformity of the detection sensitivity. Clearly, an attempt to characterize a metal detector by mapping the field strength of the transmitted electromagnetic field would be of little value because the transmitter is only half of the system. A more relevant mapping procedure is to perform a sensitivity mapping.

**Sensitivity Mapping**

There are two approaches to performing a sensitivity map. First, the object is passed through the detector passageway, and the sensitivity is adjusted to find the minimum setting required to reliably detect the object. This method assumes that the response to sensitivity relationship is linear. A more preferable method is possible when there is an interface that allows response measurements to be made. A sensitivity setting is selected that produces a strong response to the object but does not saturate the detector at any location. The test object is then passed repeatedly through the detector at each test location, and an average response is recorded for that location. The object of the mapping procedure is to locate the positions that represent the worst case for each of three detector regions: the ankle region, the waist region, and the head region. A variation of the response measurement method is to select a fixed sensitivity and to pass test targets of graduated size to find the smallest size that is detected.

#### 3.3.3.6 Periodic Field Tests

**Test Walker Movement**

For all tests the test walker should pass the target through the center of the detector arch in the region (head, waist, or ankle) that represents the worst-case location. There will be a total number of combinations equal to the number of test objects multiplied by the number of test regions. For example, if the detector is to be tested at the head, waist, and ankle regions with a total of two test objects, the total number of test combinations equals six. The walker should pause within the arch if that is normal facility operational procedure.

Extraneous motion such as nodding the head, swinging the arms, or swinging the hips should be held to a minimum. During the head test, test walkers should focus on an eye-level spot on the wall in front of them in order to keep the head from nodding.

Velocity of the walk should be a normal pace of approximately 30 inches per second as determined by a slow count (one pace per second). Velocity can range between 21 and 42 inches per second and still be acceptable.

During the ankle test, the pace of the walker should be normal with foot placement such that the ankle that carries the test target should consistently swing through the detector arch or pause within the arch, depending on which is worst case as determined by characterization testing such as the sensitivity mapping. If normal facility operational procedure dictates that persons being screened should pause within the arch, the test walker should pause in the detector arch.

### Test Preparations

It is important to know the worst-case combination of factors before beginning the field testing of a metal detector. The mapping procedure described in section 3.3.3.5 can be used to find these combinations. The combination of the factors of the worst-case target at the worst-case location in its worst-case orientation is called the absolute worst-case combination. Testing at this worst-case combination will be used to establish the probability of detection while the worst-case combinations in the other two regions can be used to verify that the detector sensitivity map has not changed. If another combination produces a response in the detector that is nearly indistinguishable from the absolute worst-case, that combination is recorded as a near worst-case.

### When to Field Test

After a worst-case target object is identified and the metal detector is set up to detect that target object in any orientation in the least sensitive region of the archway, the metal detector is ready for operation. The detector should then be tested to establish the detection rate; this number is often used to estimate the probability of detection and is determined by performing an in-performance test. The detector should also be tested to determine the detection rate whenever the metal detector environment is changed or whenever the detector is moved or serviced. The test object(s) should be used to check the detector archway at a sufficient number of points to identify any areas of low sensitivity that may have developed. A quarterly performance verification can verify that the level of operation has not changed since the installation.

### In-Plant Performance Test

The purpose of the in-plant performance test is to perform sufficient testing to estimate the probability of detection for comparison to a standard. To date, most testing performed on metal detectors has relied on attributes data (alarm/no alarm). To perform this type of testing, a target is passed repeatedly through the detector, and the number of times the detector alarms is counted. In the simplest case, the number of alarms is divided by the total number of passes. This number is the detection rate and is sometimes used as an estimation of the probability of detection. This is not very rigorous in a statistical sense. Most standards dealing with metal detector performance state a confidence level for the target probability of detection. For instance, a standard may state that the detector is to have a 0.9 probability of detection at a 0.95 confidence level. Another way of saying this is that one has a 95% confidence that the detector will detect a target 90% of the time. There are various mathematical approaches used to determine the number of times a target has to be detected by a detector to establish the probability of detection at a given confidence level; each of the methods may result in slightly different numbers due to approximations and roundoff. The following method is the most accurate.

Each pass through a detector is called a trial. Attributes testing of metal detectors is a series of Bernoulli trials. This simply means that each trial may have only one of two outcomes, in this case alarm or no alarm, and that the outcome of any trial has no effect on any other trial. This type of data follows a statistical distribution called binomial distribution. If the number of trials is large, this usually means more than thirty; an approximation can be made. In such a case the distribution can be approximated by a normal, or Gaussian, distribution. In the past this approximation was useful because the mathematics of normal distribution made it easier to calculate the required number of trials and detections. However, with the introduction of the digital computer, this advantage has all but disappeared.

Let us assume that the testing strategy is based upon allowing no more than $m$ misses out of $n$ trials. Using the mathematics of binomial distribution, an equation can be derived to calculate a confidence level. The equation is:

$$CL = 1 - \sum_{k=0}^{m} \binom{n}{k} P_d^{(n-k)} (1 - P_d)^k$$

Where CL is the confidence level, $n$ is the number of trials, $P_d$ is the probability of detection, and $m$ is the number of misses that the

testing strategy allows. The $n$ over the $k$ within parentheses is combinatorics notation that means the number of combinations of $n$ taken in groups of $k$. This can be calculated using:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

For all cases other than the number of misses equal to zero, the equation for the confidence level cannot be solved algebraically for the number of trials; however, the equation can be solved numerically with the use of a computer or a good handheld calculator.

When designing a strategy for determining the probability of detection at a given confidence level, the number of allowed misses needs to be determined by the testing organization. This number can be from zero to infinity but is usually limited by practicality to no more than two to three. This is because the required number of trials increases sharply with the number of allowed misses. If no misses are allowed, the required number of trials is held to a minimum, but the chance of failing the test is a maximum. For instance, the required number of trials for a no-miss strategy at a $P_d$ of 0.9 and a CL of 95% is 29; the required number of trials for a one-miss strategy is 46; and the required number of trials for a two-miss strategy is 61.

A popular testing method is to use a multiple strategy approach called multiple testing. This allows one to begin the testing with a maximum number of misses in mind but stop the testing at the first level where the target values for probability of detection and confidence level are met. The number of stages is the number of allowed misses plus one. If the maximum number of misses is two, there will be three stages. Because the strategy changes from stage to stage, the application of the confidence level equation becomes somewhat more complicated and results in different numbers than were obtained in the simple fixed-miss strategy. The equation for more than one miss is a single equation of more than one unknown (one unknown for each miss allowed) and therefore does not have a unique solution. The trade-off in selecting a solution is that the larger the number of trials in the first stage of testing, the lower the number of trials in subsequent stages. For example, the following solutions are possible for one allowed miss with a 0.9 probability of detection and a 95% confidence level.

If the number of trials for the first stage of testing is to be 30 (the lowest possible number of trials for the first stage must be greater than the number of trials required by the no-miss strategy for there to be a numerical solution), the number of trials required for the second stage is 28. If 32 trials are chosen for the first stage of testing, the required number of trials for the second stage drops to 20. Then, if the number of trials for the first stage is raised to 34, the number of trials for the second stage drops to 15. A typical compromise is to choose the lowest number for the first stage testing that results in a reasonable number of trials in the subsequent stages. The reason to keep the number of trials lower in the first stage is that one does not expect to reach the second stage of testing very often. For example, one may choose 32/52 as a reasonable compromise. See Table 3-1 for suggested multiple-stage test strategies. The following example illustrates the application for a three-stage (two maximum misses) test strategy based on 0.9 probability of detection and a 95% confidence level.

**Table 3-1. Number of tests required for multiple-stage performance test**

| Suggested number of alarms/number of tests as a function of stages and misses allowed. | | | |
|---|---|---|---|
| Number of Misses Allowed | Number of Stages | | |
| | 1 | 2 | 3 |
| 0* | 29/29 | --- | --- |
| 1 | 30/30 | 57/58 | --- |
| 2 | 34/34 | 51/52 | 65/67 |

*0 misses is not a multiple-stage test in the strictest sense.

Using a multiple testing approach, the total number of trials required if the detector is allowed to miss twice is 67. If, however, the detector detects the test object during each of the first 34 trials, the target values have been met. If the detector misses no more than once during the first 34 trials but detects 51 of the first 52 trials, the detector has again met the target values. If the detector misses no more than once more in the second stage (for a total of two in the first 52 trials) but detects 65 out of 67 trials, the detector passes. Failure to detect at least 65 of 67 trials results in failure of the test.

Failing the test means either that the sensitivity is not high enough or that diagnostic and corrective action needs to be taken to determine necessary changes in the metal detector environment, program, or some other factor. After test failure and corrective action, the test should be repeated.

For each of the other test combinations, the test walker should make five consistent passes. Failure to detect on any pass results in test failure and initiation of diagnostic and corrective action.

#### Weekly Performance Test

This test is intended to verify the continued normal detector operation following each in-plant performance test so that the in-plant performance test does not have to be repeated too frequently. The test configurations for this test are identical to the in-plant performance test and are a continuation of the 0.9 probability at a 0.95 confidence level strategy. The idea is to perform an in-plant performance test on a protracted schedule. By performing six trials each week, the probability of detection is reverified every six weeks. Based on a thirteen-week quarter, the probability is confirmed once per quarter by the in-plant performance test and twice per quarter by the weekly performance tests.

Each week, six passes should be made by the test walker using the absolute worst-case combination of body position and test object. One failure means that an extra twelve passes at the absolute worst-case combination should be made. Any failure in the second twelve passes, or more than one failure during the first six, constitutes a test failure, and a diagnostic and corrective action should be taken. Over the course of several weeks following a single failure to detect an absolute worst-case combination, any subsequent failure at that location within the next 30 passes will be considered a test failure. You may notice that during the protracted testing only one miss is allowed; this is because the testing routine becomes very complicated if more misses are allowed.

In addition, each week six passes will be made at one of the other combinations of body position and test object. If the test configuration is a near-absolute worst case, the same test failure logic as for the absolute worst case will apply. For all other test configurations, any failure to detect will constitute a test failure. The non-worst-case combinations that are to be tested each week should be varied in a revolving pattern until all of the combinations have been tested.

The same procedure applies for the standard SNM shielding testing. The rotating test for the other-than-worst-case combinations serves as a spot check to ensure that there are no changes to the detector's overall detection profile. The rotation testing also serves to detect changes in programming that could be the result of tampering.

#### Operation Test

A functional operation test is usually conducted at the beginning of each shift. The intent of the test is to determine that the detector is operating and will detect an obvious target. This test is performed by a person such as a guard carrying a full-sized service revolver or pistol through the detector. Failure to detect a large target indicates that diagnostic and corrective action should be taken.

### 3.3.4 Weapons Detector Search Methods

The first line of defense against unauthorized weapons is the portal metal detector. When applied correctly, a portal metal detector can provide a high probability of detecting firearms and some types of incendiary or explosive devices while maintaining a reasonable false alarm rate. A carefully thought-out procedure for weapons screening can enhance the probability of detection and lower the false alarm rate. The most important operation aspect is to ensure that people being searched move through the portal at a uniform, normal rate.

#### 3.3.4.1 Portal Weapons Search at a Controlled Area

All handcarried packages and other items should be presented for x-ray or hand inspection prior to passing through the portal metal detector. It is also advisable to encourage individuals to divest themselves of metallic items carried on their person before they pass through the detector the first time rather than wait for a false alarm. A nonmetallic container should be provided so that the items can be passed through the x-ray scanner or presented for hand search. Items removed from the person's clothing or pockets should not be allowed around the metal detector without close examination. Any item that cannot for any reason be properly searched should be prohibited.

Following an alarm, the individual who caused the alarm should be returned to the entrance of the portal metal detector and allowed to remove any metallic items that were not removed prior to the first pass through the detector. The person should then be allowed to again pass through the metal detector. If the second pass is successful (no alarm) and the items removed before the second pass have been inspected and found to be innocuous, the person should be allowed to progress to the next stage of inspection. If the second pass also fails (detector alarms again), the person should be searched using a handheld detector to isolate and resolve the alarm.

#### 3.3.4.2 Handheld Metal Detector Usage

The second line of defense in weapons search is the manual search. A useful technical aide to performing these searches is the handheld metal detector. It should be remembered that the use of the handheld metal detector alone is not always sufficient to identify the source of an alarm. For example, a handheld metal detector will alarm on a belt buckle; it will not indicate whether there is any metallic item behind the belt buckle. Asking the individual to remove the buckle or performing a pat-down inspection of the area is required to establish that the belt buckle is the only source of the alarm. A variable pitch or volume handheld detector can provide sufficient information to make that judgment.

Both types of manual searches can be facilitated through the use of a handheld metal detector. Metallic items can be located quickly by the handheld metal detector, minimizing the extent of hands-on search. The handheld metal detector should be swept over the body at a distance of no more than three or four inches in the following pattern:

(1) Starting from a shoulder, sweep down the front of the body to the ankle region, then to the other ankle and back up the opposite side of the body, ending with the opposite shoulder. If the detector's scanning coil diameter (or length) is less than half of the person's body width, the pattern will have to be modified to ensure adequate coverage.

(2) The pattern used over the front of the body should be repeated over the back of the body.

(3) Starting at one shoulder, sweep the detector coil over the outside of the arm to the bottom of the sleeve, then up the inside of the arm to the armpit. Sweep down the side of the body to the ankle, then up the inside of the leg and down the opposite leg and back up the other side of the leg. Repeat the sweep of the inside and outside of the arm opposite the side where the sweep began, ending at the shoulder.

(4) Sweep the head area and ask that all headgear be removed for search.

Particular attention should be paid to the pocket areas. Variations to this pattern are acceptable; however, care should be taken to ensure that the entire body is covered, and it is recommended that each search follow the same pattern to prevent incomplete searches.

Handheld metal detectors are sensitive and will likely sound an alarm when passed over very small metallic objects, such as jeans rivets, metal buttons and snaps, brassiere underwires, and other metallic items; for this reason a detector that has a variable intensity or pitched tone that provides some indication of the size of the metallic item that is being sensed is useful. In the hands of a skillful operator, the entire search can be performed with no actual contact with the person being scanned. If, on the other hand, the detector simply sounds a constant tone when sensing metal of any size, a pat-down of the area may be required to ensure that the item being sensed is not a firearm.

Each search should be a complete body search. Stopping the search after finding the probable cause of the portal detector alarm does not ensure that there are no other items on that person. Also, some medical surgical implants, such as knee and hip replacements, can cause portal metal detector alarms. The use of a handheld metal detector and a pat-down of the area can verify the cause of the alarm; however, it is again important to continue the search to include the entire body.

## 3.4 Explosives Detectors

### 3.4.1 Hardware Description

Weapons searches involve searches for metal that could be a firearm or an incendiary device. The only present means and techniques commercially available to screen personnel for explosives are by (1) explosives vapor detection (either personnel portal or handheld), (2) low-dose x-ray scanning, (3) hand searching, and (4) strip searching. For package/baggage screening for explosives, x-ray (transmission and/or backscatter and computer tomography) and TNA can be added. These are the only techniques or devices commercially available at the present time.

Only vapor detection devices can determine the actual presence of explosives. Other instrumental means determine the presence of a suspicious shape, area, or other anomaly, which requires further effort to confirm that the anomaly is not an explosive. Hand searching, including strip searching, perhaps can determine if an explosive is present; however, some explosives can be formed or cast into various shapes and painted, or otherwise disguised, which can complicate the visual confirmation that a material/package is an explosive.

Explosives of interest can include nitrated dynamite (ethylene glycol dinitrate-EGDN + nitroglycerine-NG), trinitrotoluene (TNT), water gels (ammonium nitrate-$NH_4NO_3$), C-4 (RDX explosive), detasheet (PETN explosive), and Semtex (RDX + PETN explosives). The latter three are termed plastic explosives in which the explosive material is combined with plasticizer material(s). The explosives of interest should be defined; this will define the sensitivity requirements for explosives detection and the appropriate explosives detection device (or system).

#### 3.4.1.1 Vapor Detection

Every explosive material has a vapor pressure. Figure 3-16 exhibits the equilibrium vapor pressure for a number of explosives materials. As can be seen, the equilibrium vapor pressures range from 64 parts per million (ppm) for EGDN ($64 \times 10^{-6}$ $cm^3$ EGDN vapor/$cm^3$ of air) to 7 parts per trillion (ppt) for RDX ($7 \times 10^{-12}$ $cm^3$ RDX vapor/$cm^3$ air). It is easier for a vapor detector to detect the more vaporous materials.

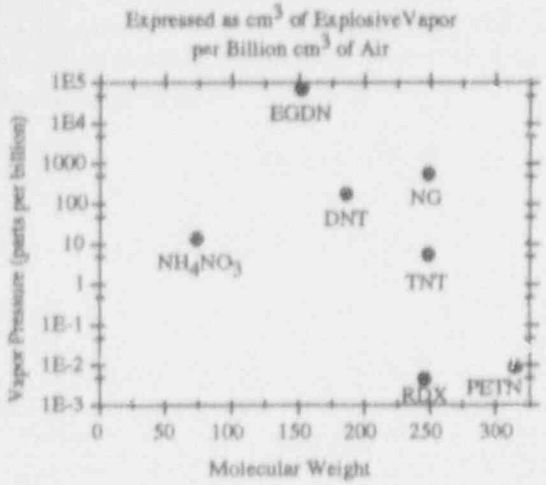



**Figure 3-16. Vapor pressure of explosives compounds**

As with any material that gives off vapors, an increase in temperature will produce a corresponding increase in vapor pressure from an explosive material. In addition, the vapors from explosives listed in Figure 3-16 possess a number of unique properties, which include (1) a proclivity to adsorb onto any material with which it makes contact (wood, plastic, glass, cloth, dust particles, and metals, both coated and uncoated), (2) a tendency to desorb upon heating, and (3) an ability to add an electron to become negatively charged (electronegativity).

Explosives material concealed under a person's clothing will emit vapors that will adsorb onto the clothing material. The vapors will diffuse through the clothing at a particular rate until they are available for detection on the surface of the outer layer of clothing. This time is termed the "soak time." The subject would have had to "wear" the explosive device for a period of time equal to the soak time before there would be any explosive vapor available for detection by an explosives vapor detection device. Heat applied to the clothing surface will increase the vapor pressure of the explosive at the clothing surface and permit its detection at an earlier time than without heating, thereby reducing the soak time. For both portal and handheld applications, the process of explosives vapor detection is divided into three parts: (1) collection, (2) preconcentration, and (3) detection.

### Collection

Any explosives vapors released from a person can be entrained (collected) in a flow of air over the outer surface of a person for a portal or over the sampling area for a handheld detector. The direction of air flow can be either horizontally across or vertically around the person.

It is desirable to utilize any method that can increase the probability of explosives vapor being released from the outer clothing surface so it can be collected in the air flow. Increasing the surface temperature helps both portals and handheld devices. Ruffling the outer clothing with a jet-blast of air helps collection in portals by dislodging vapors or particles with adsorbed explosives vapors, which can then become entrained in the collection air flow.

### Preconcentration

The flow of air used to collect explosives molecules is directed into/onto a preconcentrator designed to adsorb explosives molecules out of the air flow onto its surface(s). Subsequently, heating the preconcentrator desorbs the explosives molecules into a small volume of air flowing to the detector. Thus, the explosives molecules have been taken out from a large volume of air and desorbed into a small volume of air, i.e., preconcentrated.

A preconcentrator can be of any geometric shape, but it usually incorporates the idea of closely spaced surfaces. Silica (e.g., borosilicate glass, pyrex, fused silica, quartz) surfaces have been shown to be the best preconcentrator surfaces. For portals, the heating and cooling of the preconcentrator should be very rapid because the desired throughput is usually 10 persons/minute. Therefore, materials that can be resistively heated and that possess a high thermal conductivity frequently are used as a base, and they are coated with a thin layer of silica. The same demand for time efficiency is not required for handheld devices.

### Detection

The method utilized for detection of explosives molecules ideally depends on the sensitivity required and on the explosives to be detected. Presently available explosives vapor detection techniques include (1) gas chromatography followed by electron capture detector (GC/ECD), (2) chemiluminescence, (3) ion mobility spectrometry (IMS), (4) mass spectrometry (MS), and (5) tandem mass spectrometry (MS/MS).

ECD by itself usually is not sufficient to detect explosives molecules since it cannot distinguish between electronegative compounds. Therefore, GC/ECD is a common detection combination for some handheld and portal designs. The GC separates a composite gaseous sample into its individual

component gases, which are then fed into ECD one at a time. Determining whether explosives vapors are present is accomplished by comparing the time-response relationship to the relationships exhibited when measuring standard explosives vapor samples.

Chemiluminescence is utilized by one handheld detection system. The sample is collected onto a preconcentrator located inside a handheld suction device, which can heat the surface during sampling. After sampling, the preconcentrator is transferred into an analyzer unit, which desorbs any explosives vapors, separates them individually from the composite sample by capillary GC, and detects them separately by chemiluminescence. Like the GC/ECD, comparison with standard explosives vapors is necessary to calibrate the instrument.

IMS technology is incorporated into handheld explosives detection devices. However, these present commercial explosives detection units do not achieve the potential sensitivity of which IMS is capable. They can detect nitrated dynamite, and perhaps TNT, but are not capable of detecting the RDX in C-4 or PETN in Detasheet, or the combination of RDX/PETN in Semtex. Prototype units utilizing higher sensitivity IMS technology are being studied and should provide sensitivity for all explosives shown in Figure 3-16.

Theoretically, mass spectrometry (both MS and MS/MS) should have sensitivities comparable to, or greater than, the IMS; however, at present it is slightly less. MS is relegated to application in personnel portals since an MS unit is so large that it cannot be used in handheld explosives detection units.

#### 3.4.1.2 Personnel Portals

Explosives vapor detection personnel portals should meet the following criteria:

(1) have a uniform and sufficient air flow (either vertical or sideflow) to entrain any explosives vapors, or particles containing explosives vapors, and transport them to a preconcentrator and/or detector

(2) have a preconcentrator (if one is used) that has an efficiency factor of at least 30%, i.e., at least 30% of the explosives vapor in a sample is delivered to the detector

(3) have a throughput rate of 10 persons/minute

(4) have the demonstrated capability of detecting all explosives of interest

(5) be automated so subjective human interpretation is not required

(6) have an automatic alarm when an explosive is sensed

In addition, it is desirable for portals to:

(1) employ heating of the surface of clothing worn by a person to increase the vapor pressure of any explosive(s) present

(2) use "puffers," which ruffle the clothing surface to knock loose any explosives vapors or particles that contain absorbed explosives vapors. The "puffers" should "puff" only once or, at the most, twice

(3) have at least three sides enclosed to prevent stray air currents from affecting sample collection

Figure 3-17 illustrates a typical personnel portal device.

#### 3.4.1.3 Handheld

Handheld explosives vapor detection devices should meet the following criteria:

(1) have a uniform and sufficient air flow to entrain any explosives vapors, or particles containing explosives vapors, and transport them to a preconcentrator and/or detector

(2) have a preconcentrator (if one is used) that has an efficiency factor of at least 30%, i.e., at least 30% of the explosives vapor in a sample is delivered to the detector

(3) be applicable to both personnel and their packages, such as briefcases, lunch pails, and vehicles

(4) have the demonstrated capability of detecting the explosives of interest

(5) be automated so subjective human interpretation is not required

(6) have a self-contained gas (if necessary) and power supply, both of which will operate a minimum of six hours

(7) have an automatic alarm when an explosive is sensed

(8) be man-portable or have a sampling system that is man-portable

In addition, it is desirable for handheld detectors to employ heating of the surface of the sample area to increase the vapor

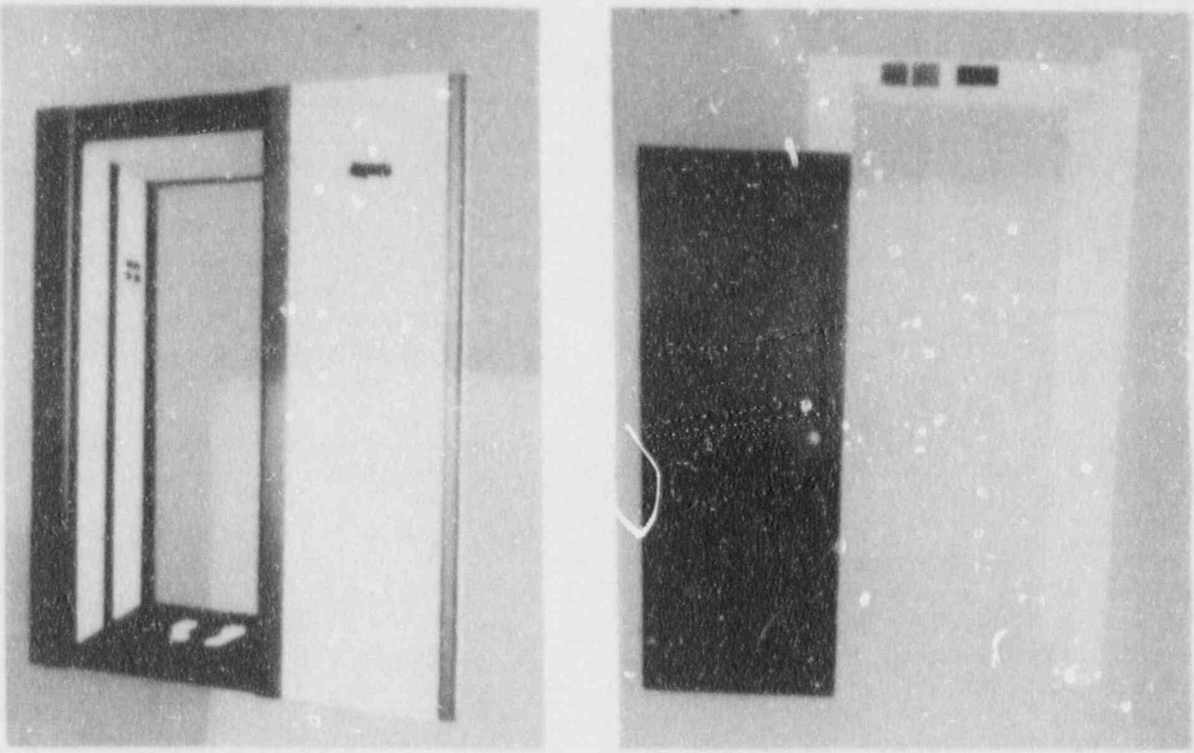


**Figure 3-17. Personnel explosives vapor detection portals**

pressure of any explosives residue present. Figure 3-18 shows typical handheld vapor detection devices.

### 3.4.1.4 Low-Dose X-Ray Scanning for Contraband

X-rays currently are used to screen packages for explosives and firearms, but a new use of x-rays is emerging, and that is checking people directly for weapons, shielded SNM, and explosives. The two x-ray processes used in explosives detection are absorption and scattering. Absorption generally is used in baggage screening, which looks at the x-rays that are not absorbed and are transmitted through the bag. For personnel screening, scattering is of primary importance, specifically what is known as "backscattering." Backscattering essentially looks at x-rays scattered back from a test subject, i.e., the x-ray source and x-ray detectors are nearly coincident.

Until recently, personnel screening for explosives could be done only by explosives vapor detection portal, a handheld explosives vapor detector, or hand searching. However, low-dose x-ray (also known as "soft x-ray" and "low-energy x-ray") scanning now is available, which can detect contraband concealed on personnel (weapons/SNM containers, explosives, drugs). This includes the gel-type explosives.

In any screening device to be used on people, safety is of prime importance. The radiation dose received while being scanned needs to be so low that it is virtually indistinguishable from background. Present scanners can scan only one side at a time. A person entering a scanner booth would have to be scanned two times, front and back, to ensure that no explosives are secreted on the person. For general use, the low-dose x-ray system should (1) be capable of processing approximately ten (10) people per minute, (2) have the demonstrated capability to discern the presence of an explosives mass of 150 g or more on a person, and (3) demonstrate a radiation output of sufficiently low magnitude that personnel will receive a radiation dose less than the permissible 100 millirem/year, which is required under NRC regulations in 10 CFR Part 20, Section 20.103 (a) (1), to be effective January 1, 1994. Ideally, the radiation dose should be <10 microrem per scan.

Making an x-ray backscattering system fully automatic is not possible at the present time. Certainly the entering and exiting of personnel, positioning of personnel to be scanned, and energizing and deenergizing the x-ray system can all be automated. However, the results of a scan are a computer-enhanced image on a display monitor showing the outline of the person and any concealed objects. Recognizing an object

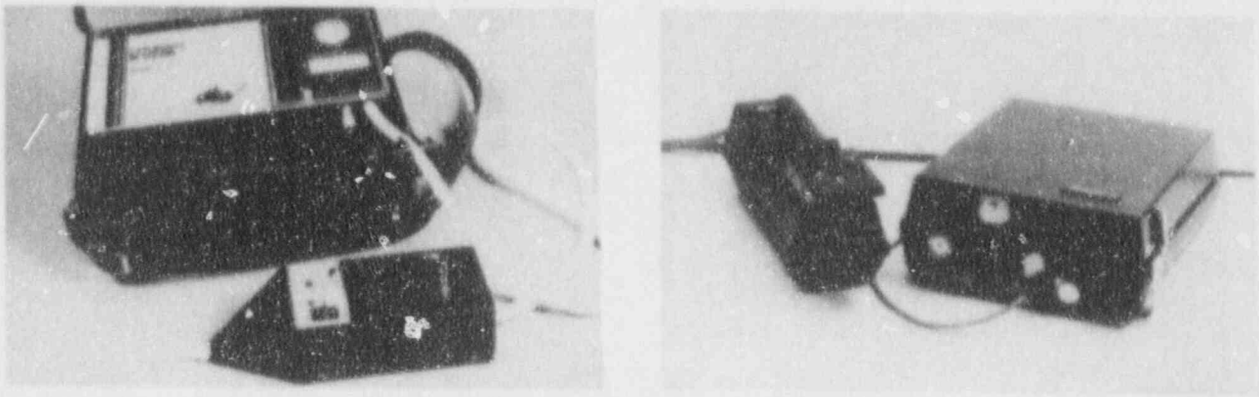


**Figure 3-18. Handheld explosives detectors**

as being suspicious and requesting further verification to determine if it is/is not an explosive is the responsibility of the operator and/or security officer. Figure 3-19 shows a typical

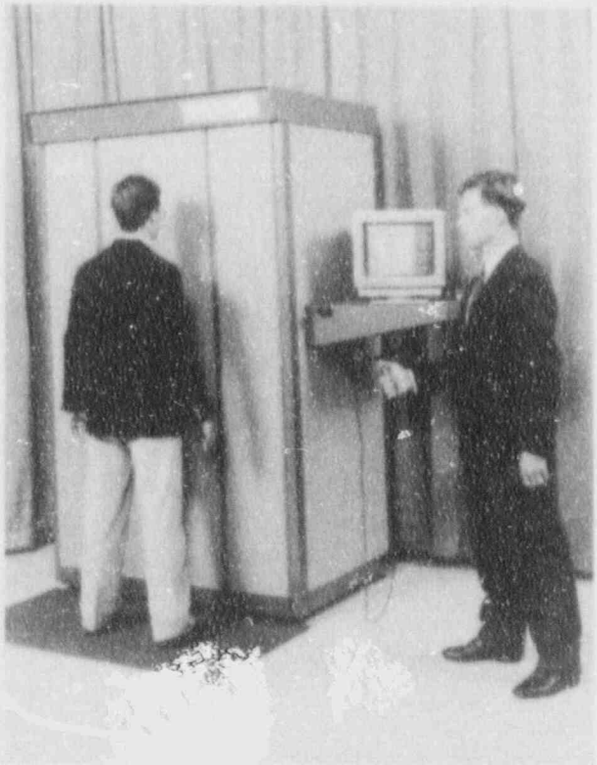


**Figure 3-19. Low-dose personnel x-ray**

low-dose x-ray personnel scanner, and Figure 3-20 illustrates a typical computer-enhanced image obtained with various materials located on the subj

### 3.4.2 Explosives Detector Installation

Vapor explosives detectors rely on the ability to collect samples of explosives vapors for analysis. The existence of new plastic explosives with extremely low vapor pressures makes the number of available explosives vapor molecules for analysis very low. Any installation feature that causes additional air currents to flow through the sample area may significantly decrease the vapor explosives detector's effectiveness. Ideally the person being searched for explosives would be in a booth, where air flow can readily be controlled. This one consideration is the single most significant environmental effect of a vapor explosives detector.

### 3.4.3 Explosives Detector Testing

This section provides an example of a testing method for determining the detection capabilities of explosives detectors. Two types of tests are described below: performance testing and operational testing.

Performance testing is designed to determine whether the detector portion of an explosives detection device (EDD) is operating in accordance with appropriate performance criteria. Performance testing should be conducted when an EDD either fails operational testing, is moved, or is adjusted. Performance testing should be done at least quarterly.

It is recommended that explosives detection devices (EDD) be capable of detecting explosives with at least a 90% effective detection rate at the 95% confidence level. This is equivalent to detecting a test sample 34 times out of 34 trials (or, if a failure to detect occurs, 51 out of 52, or 65 out of 67). (See section 3.3.3.6, In-Plant Performance Test.)

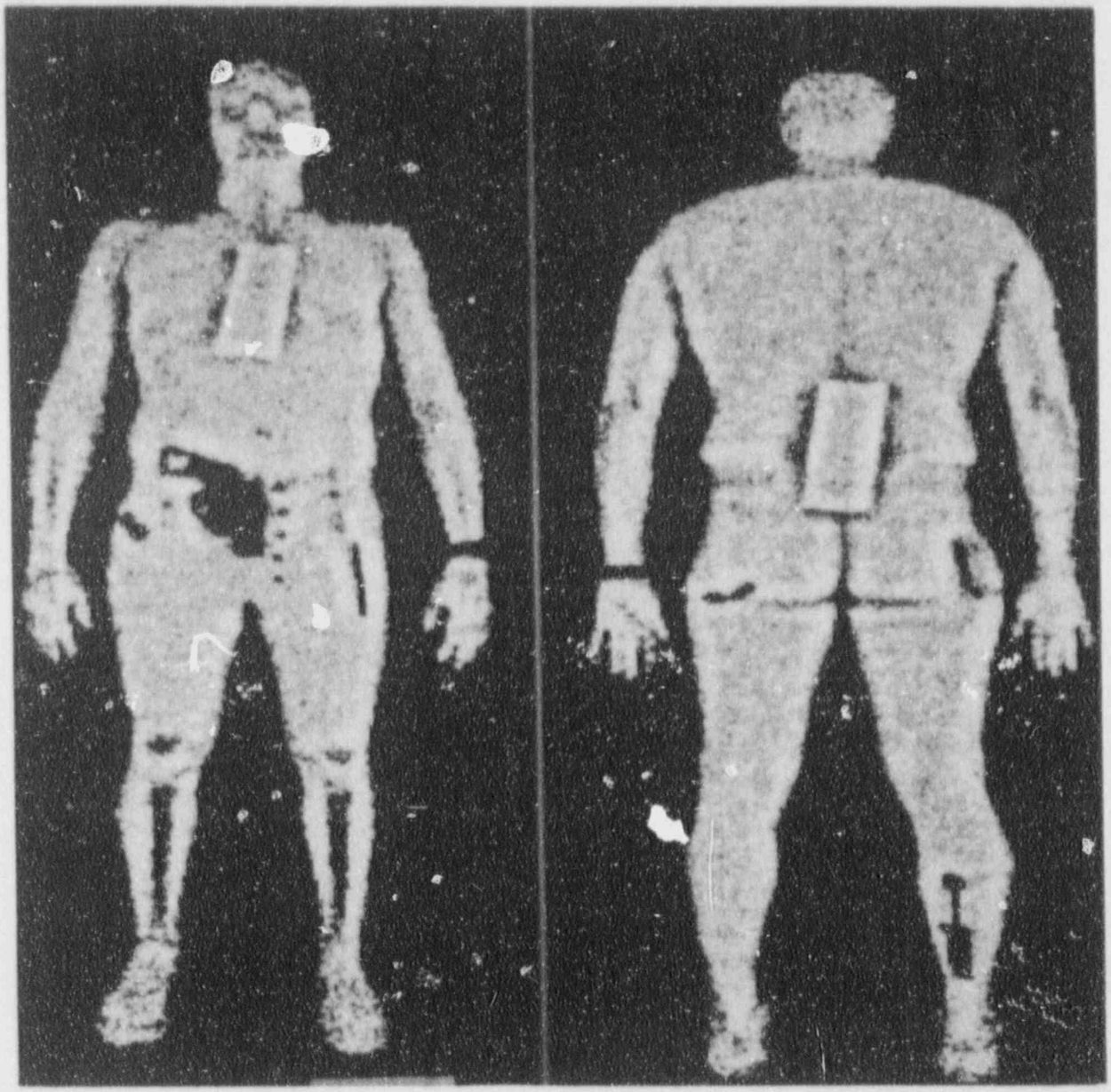


**Figure 3-20. Computer-enhanced image low-dose x-ray**

Operational testing is designed to ensure that an EDD is operating, and it is recommended that such tests be conducted whenever a unit has been turned off, when maintenance has been performed, and daily (or if possible, at the beginning of each shift). The EDD should detect a test sample three times out of three trials.

### 3.4.3.1 Personnel Portals

Performance tests are done by operating the portal without anyone or any test sample in place to ensure that no false detections are made. A calibrated vapor source is not presently available but will become available in the near future. Until that time, it is recommended that the source(s) described in the following section, Testing Vapor Source, be used. Once the calibrated vapor source is available, it should be used in place of the source(s) listed in the following section. A calibrated vapor source provides an equilibrium vapor pressure concentration of the explosive desired at the operating temperature of the booth. The output from the vapor generator is released directly into the portal's sampling air intake for a period of 5 seconds. If a positive response is not obtained, the detector is

not performing according to specifications and should be adjusted, repaired, or replaced.

**Testing Vapor Source**

The test source that has been used for portal testing in the past has been a syringe containing para-nitrotoluene in a wax solution coated on the interior of a 100-cc syringe body up to approximately the 30-cc mark; the syringe has a stop to prevent the plunger from entering the coated area. The para-nitrotoluene/wax solution should be less than one year old. The para-nitrotoluene is a simulated explosive test sample and therefore may be transported by normal means. The tip of the syringe should be kept capped when not in direct use to avoid losing the vapor. Other sources that may be considered are:

(1) a wide-mouth jar containing a 4-inch x 4-inch piece of dynamite wrapper that was taken from a stick of dynamite less than one year ago

(2) a wide-mouth jar containing at least 12 tablets of nitroglycerine heart medication that is less than one year old

(3) a wide-mouth jar containing 2-3 grams of double-base shotgun or pistol powder that was placed in the jar less than one year ago

(4) a jar containing para-nitrotoluene in a wax solution—This sample should be less than one year old

Test samples (1) through (3) are explosives test samples. The jars should be kept capped tightly at all times when not in direct use.

**Performance Testing**

The following procedures are recommended for use in performance testing of personnel portals. The portal should be operating, i.e., with air flow and detector ready. Repeat the chosen testing protocol until the detection probability of 90% at 95% confidence level is satisfied. If the desired detection probability/confidence level is not achieved, the detector is not performing according to specification and should be adjusted, repaired, or replaced.

(1) *Syringe with para-nitrotoluene/wax solution.* Remove the tip cover from the syringe tip and pull the plunger out fully to the top measuring line. Place the tip of the syringe directly in the center of, and less than one inch away from, the front of the portal's sample air intake. Depress the plunger in a slow, steady movement.

(2) *Calibrated vapor source.* Place the tip of the calibrated vapor source directly in the center of, and less than one inch away from, the front of the portal's sample air intake. Turn the vapor generator on for 5 seconds.

(3) *Test samples (1) through (4).* Remove the cap from the jar and hold the top of the jar normal to the center of, and less than one inch away from, the front of the portal's sample air intake. Hold the jar in this position for 5 seconds. Replace the cap on the jar.

**Operational Testing**

The following procedures are recommended for use in operational testing of personnel portals:

(1) First, operate the portal without anyone or any test sample in place. If a false detection is made, repeat the test; if the false detection persists, check the detector for proper operation and the portal for inadvertent contamination.

(2) Then operate the portal with a person inside the portal. If a false detection is made, repeat the test; if the false detection persists, check the portal with another person and/or without anyone inside.

(3) Operate the portal with a person in place inside the portal. The person should hold a vapor source at waist level and (a) inject vapor from the syringe into the portal at waist level; or (b) hold the calibrated vapor source at waist level and turn it on for 5 seconds; or (c) remove the lid from a jar containing a vapor source and hold it at waist level for 5 seconds.

If no detection is made, performance testing should be instituted.

### 3.4.3.2 Handheld Explosives Detectors

Performance testing for handheld explosives vapor detectors is accomplished in the same manner as for personnel portals. When a vapor generator is available, direct the output of the generator into the sampling air intake of the handheld detector for a period of 5 seconds. Until the generator becomes available, sources (1) through (3) in the above section should be used. Para-nitrotoluene can not be detected by a handheld explosives detector unless it has been adjusted to make the detection. The lid is removed from the bottle and a 5-second sample from the mouth of the jar is taken. If a positive response is not obtained, the detector is not performing according to specifications and should be adjusted, repaired,

or replaced. Operational testing is the same as performance testing in the case of handheld explosives detectors.

#### 3.4.3.3 Low-Dose X-Ray Testing

Performance testing is accomplished by placing a piece of plastic (lucite or lexan) 4 inches wide x 6 inches long x 0.5 inch thick on a subject's chest and scanning the subject. The plastic should be under at least one layer of clothing on the person. More than one person should be used as a subject in performance testing. If the tests are not successful, the system should be inspected to determine which part(s) are not functioning properly, and they should be adjusted, repaired, or replaced. Operational testing for low-dose x-ray scanners is not considered necessary if performance testing is conducted as described above.

### 3.4.4 Explosives Detector Search Methods

#### 3.4.4.1 Personnel Portal Methods

For portal explosives searches, personnel should step into the portal and place their feet on footprints outlined on the floor. They should remain in place until the operator or instrument indicates that they may proceed into the controlled area. The exit side should be locked or monitored closely by security personnel during a scan. If locked, the exit door is unlocked after no explosives are found. Personnel should not take any packages, purses, lunch pails, or other handcarried items into the portal with them. These should be given to a security officer for separate inspection.

If search equipment indicates the presence of explosives, or there is cause to suspect that an individual is attempting to introduce explosives into a controlled area, the following actions should be taken:

(1) The security officer should request that the individual empty his/her pockets and again be tested by the search equipment. If the individual complies, and after the equipment no longer indicates the presence of explosives, and the contents of the pockets have been verified as not including explosives, the individual may be allowed to pass into the controlled area.

(2) If an alarm continues to be received when the individual again is scanned by the vapor detection portal, it is acceptable to either refuse entry and conduct the individual to a holding area, or to conduct a search using either handheld equipment or a pat-down search.

#### 3.4.4.2 Handheld Explosives Detector Methods

Inspection with a handheld explosives detector should be made by one unarmed security officer while at least one other security officer observes the search. The search should be conducted by a security officer of the same gender as the person being searched. The following areas should be searched:

(1) shoulders to wrists, inside and outside the arms
(2) under upper-arm areas down side of torso to ankles
(3) insides, fronts, and backs of legs
(4) back torso from shoulders to back of pelvis
(5) front shoulder area down lower rib cage to pelvis
(6) any headwear should be removed and inspected

If an individual refuses to comply with the search, or if a firearm, explosive, or other contraband is found, entry should be denied and the person escorted to a holding area for appropriate action. If material of a suspicious or unknown nature is found, entry should be delayed until responsible security personnel are satisfied that the material is benign.

#### 3.4.4.3 Low-Dose X-Ray Methods

Personnel should step in front of the scanner unit and place their feet on the footprints outlined on the floor. They should remain in place until the operator or instrument indicates they may proceed into the controlled area. The exit side should be locked or closely monitored by security personnel. Personnel should not take any packages, purses, lunch pails, or other handcarried items into the scanner area. These should be given to a security officer for separate inspection.

If search equipment indicates the presence of an anomaly, or the licensee has cause to suspect that an individual is attempting to introduce explosives into a controlled area, the following actions should be taken:

(1) The security personnel should request that the individual empty his/her pockets and again be tested by the search equipment. If the individual complies, and after the equipment no longer indicates the presence of an anomaly, and after the contents of the pockets have been verified as not including explosives, the individual may be allowed to pass into the controlled area.

(2) If the presence of an anomaly in the scan picture continues to be observed when the individual again is scanned by the low-dose x-ray system, alternatives are to either refuse entry and conduct the individual to a holding area, or conduct a search using either handheld equipment or a pat-down search.

## 3.5 SNM Detectors

### 3.5.1 Hardware Description

The hardware used for SNM monitoring takes several forms; however, all share the same basic principles.

#### 3.5.1.1 SNM Radiation

All SNM emits radiation. This fact permits the discrimination between SNM and other materials with similar appearance. This fact also allows the use of specialized radiation detectors to monitor for the presence of concealed SNM. The types of radiation that are emitted from SNM varies according to the type of SNM, its isotopic composition, and impurities that may be present. Radiation that may be present includes gamma/x-ray, neutron, beta, and alpha emissions. Because alpha and beta radiations are very low in energy, most SNM monitors rely on gamma/x-ray and neutron detection.

#### 3.5.1.2 Detection vs Target Speed

SNM monitoring is a counting process. The longer a monitor has to perform the count, the more precise the count. The amount of time that a source is present in the monitor is dependent on the walking speed of the person carrying the source. If the person is allowed to proceed through the portal unhindered, the monitor will have only one or two seconds in which to count. If the exiting process involves procedures that cause the pedestrian to pause, such as a badge check, performing that procedure while the person is standing in the monitor will provide additional time for the monitor to perform a more accurate count. If this is inconvenient or there are no procedures that require the person to pause, turnstiles or other such devices can at least slow the person to allow more sensitive monitoring. Some automatic SNM monitors, called "wait-in" monitors, use audible tones or other devices to hold the person during the monitoring process and to signal when he/she may leave.

#### 3.5.1.3 Automatic Pedestrian SNM Detectors

Automatic pedestrian monitors are usually used as doorway monitors or pass-through monitors. The main advantage of this type monitor is that one can achieve minimum delay in a high traffic application while maintaining acceptable detection sensitivity for most situations.

#### 3.5.1.4 Handheld SNM Detectors

Handheld SNM monitoring is the easiest method to apply because no installation is required. If not already selected, a monitoring location should be chosen that is free from unnecessary interference from facility-produced radiation. Operators of these radiation detection devices should be carefully trained to properly use them. Instruments and small radioactive sources, 1μCi of $^{137}Cs$, for example, should be available during training to allow the trainees to detect a radiation intensity similar to a small quantity of SNM. Supervisors also need training so that they can effectively enforce good monitoring practices. Handheld monitors should be tested by operators or maintenance personnel on a daily basis to ensure that they detect radioactive material.

#### 3.5.1.5 Elements of a Typical SNM Monitor

The major elements of an SNM radiation monitor include a radiation detector, signal-conditioning electronics, detection electronics, decision logic/alarm annunciator, and diagnostic electronics. (See Figure 3-21.) The elements of handheld and automatic portal monitors are essentially the same. A radiation detector, which is a sensitive plastic or sodium iodide [NaI(T1)] gamma ray scintillator, responds to gamma and x-rays by producing light photons. These photons from the scintillator travel to a photomultiplier tube, either directly or through a light pipe, and are there converted to electrical signals by a photosensitive cathode. Then, electrons emitted by the cathode are amplified as a signal that reflects the amount of incident radiation and its energy.

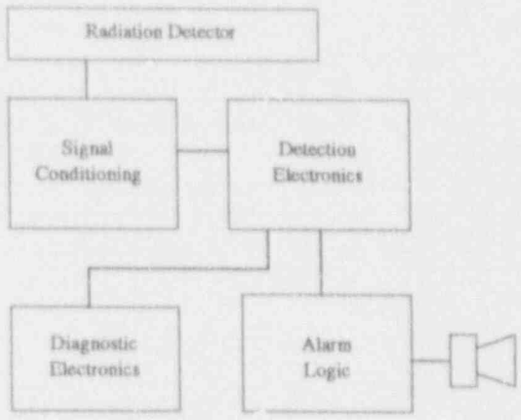



**Figure 3-21. SNM radiation monitor**

#### 3.5.1.6 Scintillation

One of the more useful interactions between radiation and matter for the purpose of radiation detection is scintillation. Through a variety of mechanisms, flashes of light are produced in scintillation material. The light is frequently in the ultraviolet region. The photons could be sensed directly, but the scintillation material can be doped with a phosphor that

converts the wavelength to one that is better matched with the spectral response of the photosensor. Because the flashes of light are low in intensity, the photosensor used in SNM monitors is a photomultiplier tube (PMT), which amplifies the light.

#### Inorganic Scintillator

Around the turn of the century there were several crystalline materials that were shown to scintillate. In 1948 it was shown that thallium-activated sodium-iodide coupled to a photomultiplier tube could be used to detect gamma rays. NaI(Tl) has become one of the most widely used materials for photon detection. Pure sodium-iodide crystals scintillate efficiently when cooled to around 77 K but lose most of that efficiency when near room temperature. The addition of thallium not only increases the efficiency at room temperature, but also causes a shift in the wavelength of the scintillation light such that NaI(Tl) is transparent to its own light. One drawback is that exposure to small amounts of moisture causes the NaI(Tl) to discolor, thus lowering its transparency to the scintillation light and making it useless for radiation detection. In recent years, the trend for portal and even handheld monitors is to use solid plastic scintillators.

#### Organic Scintillator

There are two general types of organic scintillation sensors. Liquid sensors are composed of an organic scintillator as a solute in an organic solvent. A more widely used organic scintillator is a solid solution of scintillation material. These solid organic scintillators are known as plastic scintillators. Although the efficiency of plastic scintillators is considerably lower than that of NaI(T1), their low cost and large size more than compensate for their lower efficiency. Another advantage of plastic scintillators is that they are sensitive to neutrons.

### 3.5.1.7 Signal Conditioning Electronics

In the case of the NaI(T1), the intensity of the scintillation flashes is proportional to the energy of the particle or gamma radiation (wavelength) and the spectral response of the scintillator. The flash is converted to an electrical pulse in the detection circuitry; a pulse-height discrimination circuit can then select pulses of the desired magnitude. This pulse-height filtering becomes very important when the SNM to be detected is of low intensity and emits low-energy radiation (as is the case for HEU). Conversely, the response of plastic scintillators to radiation is nonlinear. Pulse-height discrimination is still possible; however, the pulse windows are different from those for NaI(T1).

### 3.5.1.8 Detection Electronics

The process of radiation detection is a counting process. Variations in the count result in a statistical distribution known as a Poisson distribution. In this sort of distribution, the standard deviation is the square root of the background count. Increasing the count duration linearly increases the signal count while only slightly increasing the standard deviation, resulting in a better signal-to-noise ratio. During the time that the monitor is vacant, detection electronics perform repeated periodic counts to maintain an average reference background level. When a person enters the monitor, detection monitoring begins. The count from the detection monitoring is then compared against the background count. If there is significant signal above the background level (some number of standard deviations above background), an alarm sounds. There are several sampling methods that take advantage of the properties of the Poisson distribution to reduce noise, increase sensitivity, and shorten monitoring times.

#### Moving Average Method

Moving average detection is especially important for applications in walk-through portal monitors. Because the source continues to move through the monitor, it is important to sample the source signal when it is the strongest. This technique makes several overlapping tests rather than a single test. This overlapping sampling method guarantees that one of the tests will sample the source output at its most intense. Because the moving average technique tests more than once per passage, it will have more nuisance alarms per passage unless the alarm threshold is increased. Raising the alarm threshold to maintain the single-test nuisance alarm rate does not reduce the probability of detection because of the inherent higher sensitivity of this method.

#### Sequential Method

Another method for monitoring is sequential testing, which is designed to minimize the monitoring time in "wait-in" monitors. The method relies on having a variable number of tests to make its decision. It makes several short tests and typically shortens the average monitoring time considerably while maintaining the desired sensitivity. Its monitoring time varies with the perceived radiation intensity during monitoring and is extremely short for either low background intensity or strong signals. In the case where there is a high background or the SNM signal is of low intensity (the least separation between signal and background), the decision requires more tests and the monitoring time approaches the monitoring time of other methods. The sequential detection method can also be

applied to walk-through portal monitors where it has advantages similar to the moving average method.

#### 3.5.1.9 Decision Logic and Alarm Annunciation

The process of counting pulses from detected photons and deciding if there is a signal that can be distinguished above the background is performed by the alarm logic. SNM monitors typically will have both an audible and a visual alarm indication. In addition, alarm relay contacts may be provided for remote annunciation.

### 3.5.2 SNM Detector Installation

Because SNM detectors measure very small levels of radiation, anything that can be done during installation to keep the signal (SNM radiation)-to-noise (background) ratio as large as possible will enhance the detector's performance. A low-intensity constant background is the ideal situation. Detection of SNM under this situation is relatively simple. Changing background causes complications in two ways. First, during times of high background, discerning the SNM signal above the background is more difficult. Secondly, sudden upward changes in background if they are concurrent with someone passing through the monitor can cause nuisance alarms. The following paragraphs discuss considerations for SNM detector installation.

#### 3.5.2.1 Natural Background Sources

Everywhere on earth there are sources of natural radiation. The problem of detecting the presence of SNM with a monitor is distinguishing the SNM signal from the background. There are a variety of sources of natural radiation: geologic sources, interaction of the atmosphere with cosmic rays, and sources in building materials. For the most part, this background is fairly constant. However, precipitation can cause temporary increases in the background level due to radiation sources in the form of radioactive particulates that are deposited by rain or snow. During construction, a careful selection of low radiation building materials can reduce background.

#### 3.5.2.2 Artificial Sources

In the nuclear industry environment, there are radiation sources that may include emissions from the SNM being protected or from other incidental radioactive materials or radiation-producing machinery. This background may be fairly constant or may change in intensity quite suddenly. One cause of rapid change can be moving a piece of machinery that is shielding the monitor from a source, suddenly exposing the monitor to the source.

#### 3.5.2.3 Nuisance Alarm Rate Reduction Methods

One method of lowering the nuisance alarm rate is to provide a shielded room or enclosure for the monitor. If the source of SNM-produced radiation is a low-energy source, as is the case for high enriched uranium, shielding can be quite effective. If, on the other hand, the source is more penetrating, as is the case with plutonium, the shielding will be more difficult to make effective.

Since radiation is "line of sight," collimators (devices that only allow radiation to enter the detector from a single direction) installed on the detectors may be able to prevent radiation from outside the monitor from interfering with operation of the detector.

#### 3.5.2.4 Other Installation Considerations

Security is often an afterthought and, in many cases, installation of a security system is a retrofit to an existing facility. Whether the facility is new or not, one of the prime concerns when selecting a site for the installation of an SNM monitor is to find a location where the background is as low and as constant as possible. After a site has been chosen, there are several things that can be done to help ensure proper operation. If the background is relatively high, providing the monitor with a shielded room should be considered. Another concern is to provide adequate climate controls for the monitor. The climate can be controlled by either a room constructed for that purpose or cabinets for the monitor itself. Local areas of contamination may be cleaned up or shielded.

### 3.5.3 SNM Detector Testing

A comprehensive guide for the testing of SNM monitors can be found in NUREG/CR-0598, LA-7646. Some additional considerations are described below.

#### 3.5.3.1 Variables Data vs Attributes Data

The variables data available as outputs from SNM monitors far exceed that which is available from most other security equipment. The SNM monitoring industry has long recognized the value of variables testing for setup and testing of SNM monitors. In addition to the attributes data (alarm/no alarm), the monitor can provide information about the background as well as information on several parameters of the source signal.

#### 3.5.3.2 Test Object Considerations

**Gamma Radiation Test Sources**

Test sources should be used to determine the performance of SNM monitors. Ideally, the test source would be indistin-

gu[illegible]hable from the SNM being protected. It is nearly impossible to duplicate the spectral output of SNM by non-SNM sources. Even if this task were achieved, the spectral output will immediately drift due to radioactive decay of the test source isotopes. Even some SNM sources will depart from the spectral output of the protected SNM with time. The gamma ray spectrum of low burn-up plutonium changes with time as the isotope $^{241}$Pu decays to $^{241}$Am, causing a plutonium test source to increase in intensity and become easier to detect.

#### Non-SNM Sources

If tests with SNM are not necessary or are impractical, for example where a wide range of test source sizes is required, there is one commercially available isotope that can be used, with caution, as a substitute for low burn-up plutonium. The isotope $^{133}$Ba can be used for daily monitor testing and as a substitute for plutonium for some performance testing. However, $^{133}$Ba has a different gamma ray energy spectrum, and the $^{133}$Ba intensity decreases with age, unlike that of plutonium. The spectrum differences will cause different monitors to respond differently to $^{133}$Ba, even though they may respond identically to plutonium. For example, equivalent monitors for detecting HEU and plutonium would be tested with slightly different amounts of $^{133}$Ba, depending on whether their detectors are NaI(Tl) or plastic scintillator.

#### Target Shape

Other monitoring influences relate to (1) the shape of the material of interest; (2) shielding material that may be placed around SNM; and (3) the physical form of SNM. Thin sheets of material emit much more radiation from their flat surfaces than from their edges. Shielding material can cause general reduction of the radiation or act as a filter attenuating certain parts of the radiation's spectrum. Powders emit much higher levels than an equivalent amount of compact metal.

#### Shielding Effects

Absorbing material between SNM and a detector decreases the amount of radiation reaching the monitor. Shielding may take the form of material placed around the SNM to absorb gamma ray or neutron radiation, or it may simply be an object or person between the SNM and detector. Shielding that lowers SNM radiation intensity to a level below the detection threshold will permit the SNM to go undetected. For this reason, monitoring systems are most often built with detector sensitivities that are much higher than required for detecting bare SNM. High sensitivity allows detection of any transmitted gamma rays from the SNM plus any build-up radiation such as fluorescence radiation from thick lead shields. The drawback to highly sensitive monitors is that, with higher background count, the separation between the source count and the background count decreases. Therefore, in a high sensitivity mode, small variations in the background are more likely to cause an alarm if it is concurrent with someone passing through the monitor.

### 3.5.4 SNM Detector Search Methods

Individuals exiting areas where SNM is accessed should undergo SNM exit searches.

Following an alarm, the individual who caused the alarm should be returned to the entrance of the SNM monitor and allowed to again pass through the monitor. If the second pass is successful (no alarm), the person should be allowed to progress to the next stage of inspection. If the monitor alarms for a second time, a hand search should be initiated. A handheld SNM monitor can be helpful in locating the source of the alarm. If search personnel are unsure of the nature of an object or material uncovered during the search, the object or material should be confiscated and the individual's exit delayed until a determination can be made that the object or material is not SNM or does not contain SNM.

Although handheld monitors are small and seem less complex (see Figure 3-22), their functional components

**Figure 3-22. Handheld SNM monitor**

are the same as those of pedestrian and vehicle monitors. Both have a scintillation detector, a method for updating the background, sensitivity controls, and signal processing and alarm circuitry. Some differences are that it has been more common for the handheld monitors to employ NaI(T1) scintillators (although in recent years the trend is for the handheld monitors to be equipped with plastic scintillators), and the background update is manually activated on the handhelds.

Handheld SNM monitors can be very sensitive due to operating in close proximity to the source. Also, their effectiveness is dependent upon the skill of the operator. It is very important that the operators of handheld SNM monitors be well trained in their use. A search method similar to the one used for handheld metal detectors and handheld explosives detectors should be used.

## 3.6 Direct Searches

Direct searches are often required to confirm indications of contraband from more automated searches.

### 3.6.1 Pat-Down Search Methods

A hands-on search should be made by one unarmed security officer while another security officer observes the search. The search should be conducted by a security officer of the same gender as the person being searched. The following are searched by moving the hands over the clothing and the body:

(1) shoulders to wrists, inside and outside the arms
(2) under upper-arm areas down side of torso to ankles
(3) insides, fronts, and backs of legs
(4) back torso from shoulders to back of pelvis
(5) front shoulder area down lower rib cage to pelvis
(6) any headwear should be removed and inspected

If an individual refuses to comply with a hand search, or if a firearm, explosive, or other contraband is found, entry should be denied and the person escorted to a holding area for appropriate action. If material of a suspicious or unknown nature is found, entry should be delayed until responsible security personnel are satisfied that the material is benign.

### 3.6.2 Strip Search Methods

A strip search should be conducted by a security officer of the same gender as the person being searched. The person is conducted to a search room. He/she disrobes, except for underclothing, and submits his/her clothing to the security officer for inspection. The security officer also ensures that no contraband is attached to the person's body. If an individual refuses to comply with the search, or if a firearm, explosive, or other contraband is found, entry should be denied and the person escorted to a holding area for appropriate action. If material of a suspicious or unknown nature is found, entry should be delayed until responsible security personnel are satisfied that the material is benign.

### 3.6.3 Holding Area

The holding area should be an enclosed area (room) that can be entered only in the company of two unarmed security officers and one armed security officer. The two unarmed security officers should escort a person into the holding area, one on each side and one step behind the suspect. An armed security officer should be behind this trio several paces. Any procedures conducted within the holding area should be completed by this trio of security officers. One or more security officers should be on the outside of the holding area, observing the procedures through a glass portal. Exit from the holding area should be only through a second door, opposite the entrance door, which remains locked. It is unlocked only by one of the exterior observing security officers.

### 3.6.4 Testing of Pat-Down Search

Periodic testing of security personnel who are charged with performing pat-down searches should be conducted. This can be accomplished by providing three to five people, some of whom are carrying simulated explosive devices, for these security personnel to inspect through pat-down searches. If the tests are not successful, the failure should be analyzed and changes or retraining instituted.

## 3.7 Emergency Evacuations

Four concerns in emergency evacuation situations are personnel safety, unauthorized removal of SNM from the facility, unauthorized access to the facility, and accounting for the whereabouts of all personnel after the evacuation. All of these concerns can be addressed by constructing an emergency evacuation holding area. This area should be sufficiently far enough away from the facility to provide safety to those being evacuated. This holding area should not allow entry or exit until a proper accounting and search of all personnel are conducted in an orderly fashion. The holding area should be sufficiently isolated to preclude anyone handing or throwing SNM outside the area. Adherence to procedures is difficult to monitor during an emergency, so practice and training in emergency procedures using the holding area are important.

# 4 Entry/Exit Controls—Handcarried Material and Bulk Items

## 4.1 General Introduction

All handcarried items, such as purses, briefcases, packages, lunch boxes, and overcoats, should be searched separately from the personnel search. Any and all handcarried or personal items that cannot be searched properly because of construction or contents should be excluded from controlled areas. As a person proceeds through a contraband screening area, his/her handcarried items should proceed separately and be inspected for contraband at the same time he/she is being inspected. All delivered packages and bulk items should also be searched prior to being taken into controlled areas.

Since these handcarried items and bulk items are not with people, the search methods can be more active, such as using penetrating x-rays to search packages. Many packages and bulk items cannot be searched in this manner; thus, the facility relies on the effectiveness of trained security personnel conducting manual searches. The following sections describe entry and exit controls for packages and bulk items not physically on a person.

## 4.2 Hardware

### 4.2.1 Explosives Searches

All handcarried packages and bulk items should be searched for concealed firearms, explosives, or other contraband. Screening of handcarried packages can be accomplished by several methods. Listed in decreasing order of effectiveness, they are (1) physical inspection, (2) x-ray scanning, (3) thermal neutron activation, and (4) explosives vapor detection. Note that the first two techniques can detect weapons as well as shapes/materials that might be explosives, whereas the latter two cannot detect weapons. If an explosives threat is present, vapor detection can determine which explosive is present, whereas TNA can determine only that an explosive threat is present.

Handcarried packages that cannot be searched effectively by one of the above methods should be excluded from the controlled areas. Any lunch boxes, purses, thermos bottles, and other items that are to be brought into a controlled area should be opened and searched. The interiors should be inspected for contraband. The cartons containing sealed foodstuffs or beverages should be opened and searched.

#### 4.2.1.1 Physical Inspection

Physical searching can be used to determine if an explosive is present. However, some explosives can be formed or cast into various shapes, then painted or otherwise camouflaged. Therefore, the security officers conducting the search should be constantly aware of this fact. Physical inspections necessitate an appropriate place in which to be conducted. As a minimum, carpet-covered tables with adequate lighting and personnel control to keep the owner away from the search table facilitate an effective search.

#### 4.2.1.2 X-Ray Scanning

Handcarried packages or materials that cannot be readily opened or otherwise cannot be effectively searched physically should be submitted to suitable detection equipment such as x-ray.

**Principles**

The interaction of x-rays with packages or materials falls into one of two categories: transmission and backscatter. Both are used in package screening. Transmission is concerned with the x-rays, which are not adsorbed and are transmitted through the package. Backscatter refers to x-rays scattered back from a test subject, i.e., the x-ray source and x-ray detectors are nearly coincident.

Both transmission and backscatter are present when x-rays interact with material. The magnitude of interaction(s) depends on the x-ray energy, the density of the material, and the elemental composition. Generally, backscatter is considered more useful for elements such as carbon, oxygen, and nitrogen (low-Z elements). To this end, some instruments have "filters" through which part of the x-ray beam should pass prior to impinging on the target of interest. The purpose of the filter is to permit only x-rays in a particular energy range to pass. Then a comparison of interaction of both energy group x-rays with the target can be obtained. In this manner, the low-Z-containing materials can be identified and, through computer control, their image colored for easy identification. Low-Z material should be manually inspected because explosives materials are constructed of low-Z elements.

**X-Ray Detection Devices**

There are many commercial x-ray units available for use in screening packages. A schematic of a typical x-ray inspection

station for handcarried items is shown in Figure 4-1. X-ray devices for detecting explosives and other contraband should meet the following criteria:

(1) be capable of detecting a 24-gauge wire viewed under step 5 of a step wedge constructed in accordance with ASTM Standard 792-82, "Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas" for 3 out of 3 trials

(2) if a cabinet system, conform to the safety requirements contained in ASTM Standard 792-82

(3) be capable of processing 10 packages per minute

) may be single beam, single beam/dual energy, dual beam, dual beam/dual energy, and have one or multiple detectors

(5) with the unit, the operator should be able to discern if a weapon or e..plosive device is present in a typical briefcase, purse, and box

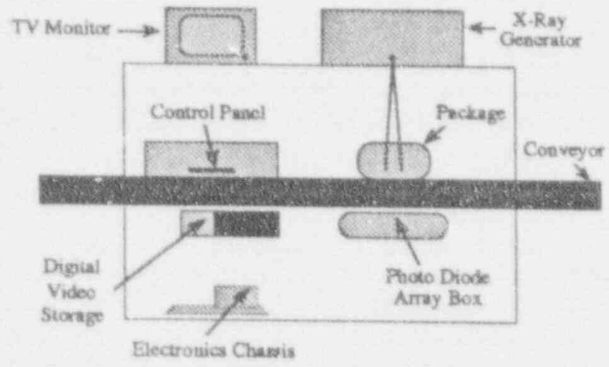



Figure 4-1. X-ray p..ckage search system

#### 4.2.1.3 Thermal Neutron Activation (TNA)

A number of nuclear techniques for detecting explosives are under study. However, the only technique that is commercially available and being used in several airports is thermal neutron activation (TNA). It is not expected that such technology will soon be used at nuclear sites because of cost and weight constraints. However, the following information is provided for completeness.

A neutron source ($^{252}Cf$) provides thermal neutrons that will interact with various elements, including nitrogen. The interaction is $^{14}N$ + neutron ——> $^{15}N$ + gamma ray. The gamma ray is termed a prompt gamma emitted at the time $^{14}N$ absorbs the neutron—the gamma ray is not a decay gamma. This prompt gamma ray possesses a specific high energy that can be detected with sodium iodide (NaI) detectors. Through computer processing, the area of interaction of the thermal neutrons with nitrogen can be displayed. The explosives shown in Figure 3-16 have a very high nitrogen content. Therefore, a high area of thermal neutron interaction with nitrogen is suspect as an explosive. Of course, the nitrogen in any nitrogenous material will interact with the neutrons and provide a high nitrogen density area on the computer display. However, not many materials have the nitrogen density that the explosives possess.

Associated with the TNA is a transmission x-ray system that is activated to look at any package that exhibits a high neutron density. This combined system is termed XENIS (X-ray Enhanced Nuclear Interrogation System). The XENIS tries to determine if any correlation exists between the high nitrogen density area and any suspicious areas in the x-ray image.

#### 4.2.1.4 Vapor Detection

The principles of vapor detection are discussed in Section 3.4.1.1. Personnel portals are not suitable for package inspection, but handheld explosives vapor detection devices can be used.

The criteria for handheld devices are described in Section 3.4.1.3.

## 4.3 Testing of Entry/Exit Control Systems for Packages and Bulk Items

### 4.3.1 Testing of X-Ray for Packages

Performance testing should consist of demonstrating that the x-ray detector system is capable of detecting a 24 American wire gauge viewed under step 5 of a step wedge constructed in accordance with American Society of Testing and Materials (ASTM) Standard 792-82, "Standard Practice for Design and Use for Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas." Operational

testing for x-ray systems may not be considered necessary if performance testing is conducted as described.

## 4.4 Methods for Entry/Exit Control for Packages and Bulk Items

As a person proceeds through a portal or contraband screening area, his/her handcarried items should proceed separately and be inspected for contraband at the same time he/she is being inspected.

All material, packages, and bulk items should be searched for concealed firearms, explosives, or other contraband. Handcarried deliveries, such as foodstuffs and beverages, should be identified and verified as authorized delivery prior to entry. All such materials and packages should be searched for firearms, explosives, and other contraband. Packages holding foodstuffs and beverages should be subjected to search. For items in which size, weight, packaging, or other physical characteristic prohibits effective search, specific regulatory requirements should be consulted.

### 4.4.1 Physical Inspection Methods

Physical inspection refers not only to package inspection, but also to behavior of personnel, i.e., profiling. A person behaving furtively or being hesitant to subject himself/herself or his/her package(s) to inspection are considered suspect. A package should not be accepted for inspection unless the person will go through inspection himself/herself at the same time. If an individual refuses to comply with the procedures, or if a firearm, explosive, or other contraband is found, entry should be denied and the person should be escorted to a holding area for appropriate action. If material of a suspicious or unknown nature is found, entry should be delayed until responsible security personnel are satisfied that the material is benign.

Only packages that can be opened should be presented to a security officer for physical inspection, and they should be open. The officer looks at the package interior to determine if any object/shape appears anomalous. Objects should be inspected both manually and visually to ensure that they are not explosives or other contraband. The interior of the package is searched for hidden contraband. The interior of any radio, computer, calculator, or other electronic equipment should be inspected. These items should be demonstrated to the officer to be operable. The interior surface of the package/bag should be inspected to determine if contraband is concealed in the top/bottom/sides of the package.

### 4.4.2 X-Ray Search Methods

Under optimal conditions, two individuals should operate an x-ray scanner. One should assist personnel in orienting their packages properly onto the conveyer belt. The other should operate the x-ray scanner. The scanner operator should not be in position more than 30 minutes at a time because his/her ability to recognize contraband in the display image is compromised after that period of time. Therefore, the two operators should switch positions approximately every 30 minutes and be assigned other duties for at least 15 minutes. This is explained in ASTM F792-88, Appendix X2.

Each package should be placed on its side in the center of the x-ray conveyor and passed through the x-ray scanner. If the image reveals any shape, coloration, or other factor that may be contraband, procedures should be defined to:

(1) pass the package through the x-ray scanner again

(2) reverse the package, i.e., flip it over, and pass it through the x-ray scanner again

(3) physically inspect the package

(4) call a security inspector to accompany the person and package to the holding area, if necessary

If an individual refuses to comply with the procedures, or if a firearm, explosive, or other contraband is found, entry should be denied and the person should be escorted to a holding area for appropriate action. If material of a suspicious or unknown nature is found, entry should be delayed until responsible security personnel are satisfied that the material is benign.

### 4.4.3 Vapor Detection Methods

Packages and bulk items may be searched for explosives with a handheld explosives detector. The following general method should be followed:

(1) Scan the surface of the package, purse, or other object.

(2) The package should be opened; scan the interior in the manner authorized by the detector manufacturer, being certain to scan into pockets and other recesses within the package.

(3) If unable to open the package, scan along any holes or other openings into the package and along seams.

(4) If dissatisfied with ability to obtain a good sampling, or there is cause to suspect that an individual is attempting to introduce explosives into the controlled area, the person and his/her package(s) should be taken to an x-ray scanning station.

If an individual refuses to comply with the procedures, or if a firearm, explosive, or other contraband is found, entry should be denied and the person should be escorted to a holding area for appropriate action. If material of a suspicious or unknown nature is found, entry should be delayed until responsible security personnel are satisfied the material is benign.

# 5 Entry/Exit Controls for Vehicles

## 5.1 General Introduction

Vehicles should be searched for unauthorized personnel, firearms, explosives, and incendiary devices prior to their entering a controlled area. The search should include the cab (both front and back seats of a sedan/convertible), engine compartment, undercarriage, and cargo area. (Refer to NUREG/CR-0485, "Vehicle Access and Search Training Manual" for details.) Emergency vehicles and emergency response personnel allowed facility access without search should be escorted while onsite.

The vehicle searches should generally be conducted in a portal or monitoring station and are generally manual searches by trained security officers. These searches and the search aids are described below.

## 5.2 Hardware

All material, packages, and other cargo carried by any vehicle should be searched for firearms, explosives, and other contraband prior to entry into a controlled area. Screening of material and bulk items carried by vehicles can be accomplished using the same hardware and procedures described in Section 4.

### 5.2.1 Contraband Search Hardware

Three methods can be considered to search vehicles for explosives and firearms: (1) a handheld explosives detector, (2) a physical, e.g., hand, search, and (3) a canine search. The use of hardware in a vehicle search is limited; however, explosives vapor detectors and canines can be used to screen for explosives.

### 5.2.2 SNM Vehicle Monitors

There are two types of vehicle SNM monitors in use. The technology of the vehicle monitors is basically the same for the pedestrian monitors. The two types of vehicle monitors are analogous to the two types of pedestrian monitors. The portal vehicle monitor is similar to the walk-through monitor in that the vehicle is not required to remain stationary for extended periods of time. Vehicle portals are used only where relatively large quantities of SNM, or highly radioactive forms of SNM, need to be detected. The vehicle monitoring station, on the other hand, requires the vehicle to remain stationary during the time that monitoring is taking place. In both cases inductive loops in the roadway can take the place of the break beam or other such devices used as occupancy sensors for pedestrian monitors.

## 5.3 Installation Considerations

Vehicles should be inspected prior to entering a controlled area, and they should be inspected for SNM upon leaving an area where SNM is accessible. These inspections, in most instances, occur in a vehicle portal at the area boundary. The location and installation of these portals is important to ensure an effective screening process.

### 5.3.1 Vehicle Portal Monitors

During a search for radioactive material, vehicle portals operate best when background radiation intensity is relatively low and constant. Collocation of the monitor with other processes that cause the vehicle to pause, such as a badge check, can provide additional time for monitoring. In any case, the location of the radiation monitor should be where the vehicle passes close to the monitor panels, and the vehicle should move slowly. Fences and speed bumps can assist in achieving this goal.

### 5.3.2 Vehicle Monitoring Stations

Vehicle monitoring stations are used where the highest sensitivity to radioactive material is required. High sensitivity is achieved by positioning detectors as close to vehicles as possible, analyzing data from small groups of detectors to maximize the importance of a diversion signal, and counting for the longest practical period of time. Vehicle monitoring stations require more construction than do other vehicle monitors. A framework is needed to support the overhead detectors, and trenches are needed for below-vehicle detectors. Occupancy can be detected with a roadway vehicle detector loop or other device.

## 5.4 Methods for Entry/Exit Control for Vehicles

The first step in screening vehicles in all cases is to turn off the vehicle's engine. Additionally, the security officer may ask the driver to hand the ignition keys to a security officer. Searching for explosives on a vehicle is best performed in an enclosed area where airflow is controlled.

## 5.4.1 Handheld Explosives Vapor Detector Methods

The four sections of a vehicle should be examined in the following manner.

#### 5.4.1.1 Engine Compartment

Run the sampler (or sampling portion of the detector) over the entire interior surface of the hood, using a slow, sweeping motion. If a swipe sample is necessary, run the swipe over the interior surface of the hood. Inspect the entire engine compartment on and around the engine in the same manner with the handheld vapor detector.

#### 5.4.1.2 Driver/Passenger Area(s)

With a handheld explosives detector (or swipe), sample under the total dashboard area, glove compartment, seatback(s), seat(s), and under the seat(s) on all sides. Sample the seating area in the rear of the vehicle in the same manner as the front. In all cases, sample in the crack where the seat and back come together.

#### 5.4.1.3 Trunk (Bed of Truck)

With a handheld explosives detector, sample the total interior surface of the trunk, including the trunk lid, under any rags, blankets, or other coverings in the trunk, wheel wells, the back and underside of the rear seat, the spare tire, and the area where it is located.

#### 5.4.1.4 Undercarriage

The undercarriage is difficult to survey with a handheld explosives vapor detector in a normal manner. One option is to have a pit or ramp over which the vehicle is parked. A security officer in the pit can then inspect the undercarriage with a handheld explosives detector. In the front of the pit area should be a vehicle barrier in the up position. If the inspection reveals no contraband material, the barrier is then dropped and the vehicle may proceed. If contraband is discovered, security personnel will take the vehicle, driver, and other occupants to a holding area.

## 5.4.2 Physical Search Methods

Physical examination of the four sections of a vehicle can be accomplished in the manner described below. Security personnel should have the driver (1) open the engine hood; (2) provide access to the vehicle's rear portion, i.e., open the trunk lid, open the door to the camper shell; and (3) open any closed areas inside the vehicle, e.g., glove compartment.

#### 5.4.2.1 Engine Compartment

The security officer should look at and feel the entire interior surface of the hood. He/she should also visually inspect the entire engine compartment, including the engine.

#### 5.4.2.2 Driver/Passenger Area(s)

The security officer should visually and with hands inspect under the total dashboard area, glove compartment, the top(s) of seat(s), the seat(s), and under the seat(s) on all sides. The same should be done for a seating area in the rear of the vehicle. In all cases, the security officer should feel with a hand between where the seat and back come together.

#### 5.4.2.3 Trunk (Bed of Truck)

The security officer should look at and feel with hand(s) the total interior surface of the trunk, including the trunk lid, under any rags, blankets, or other coverings in the trunk, wheel wells, the back and underside of the rear seat, the spare tire, and the area where the spare is located.

#### 5.4.2.4 Undercarriage

The undercarriage can be surveyed using one of the following to provide access to the undercarriage.

**Pit or Ramp Inspection**

A pit or ramp should be available over which the vehicle should park. A security officer can then inspect the undercarriage. In the front of the pit or ramp area would be a vehicle barrier in the up position. If the inspection reveals no contraband material, the barrier is dropped and the vehicle may proceed. If contraband is discovered, security personnel will take the vehicle, driver, and other occupants to a holding area.

**Inspection with a Mirror**

If a pit or ramp is not possible, a small hand-dolly on which a mirror(s) is attached can be used. The dolly is pushed under the vehicle, and the mirror permits security personnel to inspect the undercarriage. The dolly should be rolled back and forth, from front to back of the vehicle, from both sides of the vehicle, while security personnel observe the undercarriage in the mirror(s). The security personnel should inspect the undercarriage carefully. The vehicle barrier in front of the vehicle should remain in the up position until cleared by the security officers. Since the undercarriage area is the most difficult to inspect, it is a likely place for an adversary to conceal contraband.

## 5.4.3 Canine Search Methods

### 5.4.3.1 Limitations

Canines may be capable of providing a satisfactory detection capability for explosives in vehicles or in oversized packages in the vehicles. If used, they should be trained, used, and retrained at least weekly in accordance with recognized procedures to ensure continued capability and reliability. Any training samples should be independently verified that they are not contaminated. Since any animal may present unpredictable problems and weaknesses, other detection devices or equipment should be immediately available to serve as backups in the event of a dog's illness or other type of abnormal behavior. Canines trained for explosives detection should not be used for detection of controlled or illegal chemical substances and vice-versa.

### 5.4.3.2 Testing

Testing of canines should be done only with real explosives samples. If testing is possible, every precaution should be taken to ensure that no cross-contamination of the explosives test samples has occurred. Also, the explosives handler should wear double gloves when handling explosives, and another person should open, close, and seal the box or vehicles. The exterior of the box or vehicle should not become contaminated with explosives. At no time should the canine handler touch the explosives test samples or the container to be used in the tests.

The test should include at least ten boxes or vehicles. Boxes could be briefcases, lunch boxes, purses, or cardboard boxes. Randomly load one-half of the boxes or vehicles with explosives test samples and arrange the empty and loaded tests in a row in random order with ten-foot spacing. The dog and handler may go down one side of the row, allowing the canine to inspect the boxes or vehicles, and return up the other side. A satisfactory test would be if all samples were located. This kind of performance is well within the capability of a trained and effective canine/handler team.

# 6 Bibliography and Standards

## 6.1 Bibliography


Dionne, B. C. et al., *J. Energetic Matls.*, 4, 447, 1986.

Dobratz, B. M., and P. C. Crawford, *LLNL Explosives Handbook, Properties of Chemicel Explosives and Explosive Simulants, UCRL-5299? Change 2*, Lawrence Livermore National Laboratory, January 31, 1985.

Hannum, D. W., "Characteristics of Select Glass Tube Preconcentrators Used With an Ion Mobility Spectrometer," Sandia National Laboratories, SAND89-0242, April 1989.

Henderson, M. A., T. Jin, and J. M. White, "The Desorption and Decomposition of Trinitrotoluene Adsorbed on Metal Oxide Powders," *Appl. Surface Sci.*, 27, 127-40, 1986.

Holmes, J. P., L. J. Wright, and R. L. Maxwell, "A Performance Evaluation of Biometric Identification Devices," Sandia National Laboratories, SAND91-0276, June 1991.

Kenna, B. T., and, F. J. Conrad, "Studies of the Adsorption/ Desorption Behavior of Explosive-Like Molecules," Sandia National Laboratories, SAND86-0141, October 1989.

Kenna, B. T., and D. W. Murray, "Evaluation Tests of the SECURE 1000 Scanning System," Sandia National Laboratories, SAND91-2488, February 1992.

Meyer, Rudolf, "Explosives," *VCH*, Weinheim, FRG, 1987.

Porter, L. K., L. R. Gallo, and D. W. Murray, "Metal Detector Technology Data Base," Sandia National Laboratories, SAND90-1719, August 1990.

White, R. J., "Electromagnetic Shielding Materials and Performance," Don White Publishing, Gainesville, Virginia, 1986.


## 6.2 Standards

The history of standards for SNM detectors has been one of change and development. Some of the documents published in the past that addressed this subject include the following:

1. Regulatory Guide 5.7, sections 5.7.3 and 5.7.4, *Directorate of Regulatory Standards*; United States Atomic Energy Commission; June 1973.

2. *Sandia Entry Control Handbook* quoted requirements found in AECM-2405 (and appendix). The date of the handbook is June 1980.

3. The Los Alamos National Laboratory published a document in 1979 (NUREG/CR-0598, LA-7646; "On Site Inspection Procedures for SSNM Doorway Monitors") that contains a proposed draft revising NRC regulatory guide 5.27.

4. Early in 1987, a draft of the *United States Department of Energy Safeguards and Security Standards and Criteria* was circulated. It contains proposed standards for SNM detectors. In each case, the criteria referenced *ERDA Personnel Doorway Monitor Standards* A-2-75-298, 3/5/78, which is a Los Alamos document actually published in 1975.

5. NILE&CJ Standard for Walk-Through Metal Detectors For Use In Weapons Detection, U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. (Note: This standard was written in 1974, and many of the tests described are appropriate only for passive or continuous wave metal detectors. Passive metal detectors are no longer used for security applications, and the majority of portal metal detectors in use today are pulse type; therefore, this standard should be applied with care.)

In addition to the above, the American Society for Testing and Materials (ASTM) has been developing application guides and test methods for radiation monitors. This is being done by a subcommittee (C26.12) of Committee C-26 on nuclear fuel cycle. In addition to the published standards, there are draft documents dealing with both SNM and portal metal detectors. Four are published and include:

ASTM Standards on SNM monitoring in the 1991 Annual Book of ASTM Standards, Vol. 12.01.

C1112 Guide for Application of Radiation Monitors to the Control and Physical Security of Special Nuclear Material (1988), pp. 661-668

C1169 Guide for Laboratory Evaluation of Automatic Pedestrian SNM Monitor Performance (1991), pp. 713-721

C993 Guide for In-Plant Performance Evaluation of Automatic Pedestrian SNM Monitors (1990), pp. 453-458

C1189 Guide to Procedures for Calibrating Automatic Pedestrian SNM Monitors (1991), pp. 747-755

# GLOSSARY

The glossary includes words having specialized meanings, technical terms, units, initialisms, abbreviations, and acronyms used in this NUREG.

*access control* means the portion of an entry-control system that verifies authority and authorizes access of personnel seeking entry into a controlled area.

*access delay* See delay.

*activation (neutron activation)* means bombarding a material with neutrons to produce radioactive atoms.

*adversary* means an individual or group attempting to steal special nuclear material or perform radiological sabotage; an adversary may be an insider or outsider.

*alarm* means a warning from a sensor or sensor system, usually signaled by light or sound; it may indicate a false alarm, nuisance alarm, or valid alarm.

*Am* means Americicium

*antipassback* means an entry-control system capability wherein the authorizing credential, such as a badge or pass, is controlled physically or procedurally, thus preventing the credential from being used twice for entry without an intervening exit.

*assessment* means the determination of the cause of an alarm and the extent of the threat.

*Ba* means Barium

*Cf* means Californium

*Ci* See Curie.

*cm* means centimeter (10-meter).

*communication* means the function of transmitting or interchanging information, including both transmission of alarm signals to a central processing station and transmission of response information to security personnel.

*communications system* means the equipment and procedures used by the security force for sending and receiving messages.

*contraband* means materials such as weapons, explosives, or incendiary devices that are not permitted to enter a particular area.

*Curie (Ci)* means a unit of radioactivity (3x10-disintegrations per second).

*deceit* means attempt to defeat a security system using false identification or authorization.

*delay (access delay)* means slowing down an adversary's progress.

*detection* means determining that an unauthorized action has occurred or is occurring; detection includes sensing the action, communicating the alarm to a control center, and assessing the alarm. (Detection does not exist without assessment.)

*DOE* means United States Department of Energy.

*duress* means the condition of a guard who is under attack or held hostage by an adversary.

*ECD* See electron capture detector.

*EDD* means explosives detector device.

*EGDN* means ethyleneglycol dinitrate. Also known as nitroglycol; utilized in mixtures with nitroglycerine (NG) because it markedly decreases the freezing temperature of NG and decreases the sensitivity of nitrated dynamite to shock.

*electron capture detector (ECD)* means a passive explosives vapor detector.

*element* means a distinct part of a physical protection system.

*EMI* means electromagnetic interference.

*encryption* means in digital communications, encoding an intelligible binary data stream to prevent unauthorized eavesdropping of radio transmissions.

*entry control* means the equipment and procedures used to verify access authorization and to detect contraband and nuclear materials; generally considered part of the physical protection function of detection.

*facility safeguards system (safeguards)* means a system to protect against the removal of special nuclear material and the release of radioactive material beyond the facility's boundary. It is often subdivided into a physical protection system and a material control and accounting system.

*false alarm* means an alarm normally associated with electronic malfunction of the sensing device.

*ferromagnetic* means that a material has a relative permeability that is much greater than 1. Ferromagnetic metals are strongly attracted by a magnet.

*fuel cycle* means the sequence of basic operations involved in the production of electrical energy from nuclear fuels.

*GHz* means gigahertz ($10^9$ hertz).

*hertz (Hz)* means a unit of frequency (1 cycle per second).

*Hz* See hertz.

*IMS* See ion mobility spectrometer.

*ion mobility spectrometer (IMS)* means a time-of-flight mass spectrometer that measures the mobility of ions at atmospheric pressure; a passive explosives vapor detector.

*kHz* mean kilohertz ($10^3$ hertz).

*MAA* See material access area.

*material access area (MAA)* means a location in a nuclear facility where a person can have access to nuclear material with an opportunity for theft.

*MHz* means megahertz ($10^6$ hertz).

*NAR* means nuisance alarm rate. (See nuisance alarm.)

*nonferromagnetic* means that the material's relative permeability is equal to 1. Nonferromagnetic metals are not attracted by a magnet.

*NRC* means United States Nuclear Regulatory Commission.

*nuclear material* means any fissile or fertile material used in nuclear reactors.

*nuisance alarm* means an alarm that occurs when the sensing device is operating normally but that is not caused by an unauthorized action. For example, wind, snow, or birds may cause nuisance alarms.

*PA* means protected area.

*permeability* means the propety of a substance that determines the degree in which it modifies the magnetic flux in the region occupied by the substance in a magnetic field.

*PETN* means a solid explosive.

*physical protection* means measures for the protection of nuclear material or facilities designed to prevent unauthorized removal or sabotage.

*PIN* means personal identification number.

*positive personnel identity verification* means examination of a unique physical characteristic, such as voice, eye pattern, or fingerprint, of a person to compare with stored data. If the data match, the person's identity is verified.

*PPS* means physical protection system.

*protected area* means a specifically defined area, enclosed by one or more physical barriers, to which access is controlled.

*Pu* means plutonium.

*RDX* means a solid explosive.

*real-time* means an observation made at the time an event is taking place.

*relative permeability* means the permeability of a substance divided by the permeability of free space.

*response* means the act of alerting, transporting, and staging a security force to intercept the adversary and stop him before his goal is achieved.

*response force* means the guards that respond immediately to counter the threat of an adversary.

*RF* means radio frequency.

*safeguards* See facility safeguards system.

*scintillation* means the process by which photons are produced as a result of the absorption of ionizing radiation in scintillating material; used in nuclear material detectors to detect gamma and x-rays from the radioactive decay of special nuclear material.

*sensor* means a device that responds to a stimulus associated with an unauthorized action, such as an intrusion into a protected area or an attempt to smuggle contraband through an entry.

*site* means the space of ground occupied by a facility or plant.

*SNM* See special nuclear material.

*special nuclear material (SNM)* means uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium.

*surveillance* means the collection of information through devices and/or direct observation in order to detect undeclared movements of nuclear material, tampering with containment, falsification of information related to locations and quantities of nuclear material, and tampering with IAEA safeguards devices.

*tamper* means to interfere in an intentional, unauthorized, or undeclared manner to physically defeat a security device.

*theft* means the unauthorized removal of special nuclear material or other valuable material from a facility.

*thermal neutron activation* means an active method of explosives detection.

*throughput* means the rate at which material is processed in a facility or the rate at which people pass through an entry-control portal, a contraband detector, or an SNM detector.

*TNT* means trinitrotoluene, a solid explosive..

*trade-off* means a balancing of factors, all of which are not attainable at the same time; giving up one thing for another.

*transducer* means a device that converts one form of energy to another form of energy.

*VA* means vital area.

*vital area* means an area of a plant or facility containing equipment or material whose failure, destruction, or release could directly or indirectly endanger the public health or safety by exposure to radiation.

**Distribution**

Carol Whiddon
BE Inc.
P.O. Box 381
Hwy 278W, Airport Industrial Park
Barnwell, SC 29812

6400 N.R. Ortiz
6405 D.A Dahlgren
9500 D.S. Miyoshi
9504 R.W. Moya
9543 J.C. Matter (2)
9548 J.F. Chapek
9548 J.P. Holmes (2)
9548 B.T. Kenna (2)
9548 D.W. Murray (2)
7141 Technical Library
7151 Technical Publications
8523-2 Central Technical Files

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

# BIBLICGRAPHIC DATA SHEET

*(See instructions on the reverse)*

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, If any.)

NUREG/CR-5899

SAND92-1339

2. TITLE AND SUBTITLE

Entry/Exit Control Components for Physical Protection Systems

3. DATE REPORT PUBLISHED

MONTH: November

YEAR: 1992

4. FIN OR GRANT NUMBER

L1387

5. AUTHOR(S)

J.F. Holmes, B.T. Kenna, D.W. Murray

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION – NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Sandia National Laboratories
Albuquerque, New Mexico 87185

9. SPONSORING ORGANIZATION – NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

Division of Safeguards and Transportation
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

The purpose of this report is to provide technical information on the major components of entry control systems: identify verifiers, weapons detectors, explosives detectors, and special nuclear material (SNM) detectors. For each type of device, information is presented on principles of operation, hardware features, recommended installation, testing methods, and operational procedures. Applications to personnel, handcarried packages, bulk items, and vehicles are addressed.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Nuclear Safeguards
Entry Control
Identity Verifier
Contraband Detector
Explosives Detector
SNM Detector
Physical Protection
Weapons Detector

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)

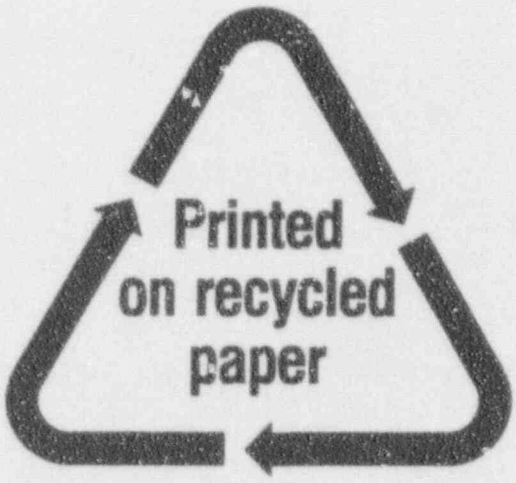
Unclassified

(This Report)

Unclassified

15. NUMBER OF PAGES

16. PRICE




Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67