Carcass Disposal: A Comprehensive Review

National Agricultural Biosecurity Center Consortium
USDA APHIS Cooperative Agreement Project
Carcass Disposal Working Group

August 2004

Chapter

13

Physical Security of Carcass Disposal Sites

Authors:

Darryl D. Drayer — International Environmental Analysis, Sandia National Laboratories
John L. Russell — Intrusion Detection Technology, Sandia National Laboratories

Supporting Authors/Reviewers:

Kimberly Asbury — Intrusion Detection Technology, Sandia National Laboratories
Randall Phebus — Animal Sciences & Industry, Kansas State University

Table of Contents

Abbreviations

A	active (Table 2)
C	covert (Table 2)
CCTV	closed-circuit television
CDC	Center for Disease Control and Prevention (Table 1)
FAA	Federal Aviation Administration (Table 1)
IR	infrared
L	line (Table 2)
LOS	line of sight (as in line-of-sight sensors) (Table 2)
NAR	nuisance alarm rate
NAR (OR)	nuisance alarm rate of the OR combination
P	passive (Table 2)
P_D	probability of detection
P_D (AND)	detection probability of the AND combination
PIR	passive infrared
PPS	physical protection system (Figure 1)
TF	terrain-following (as in terrain-following sensor) (Table 2)
USDA	United States Department of Agriculture
V	visible (Table 2)
VMD	video motion detectors
VOL	volumetric (Table 2)

Section 1 – Key Content

1.1 – Overview

Serious issues mandate the need for a security system during carcass disposal operations. Relatively high-value equipment may be used in the operation that would be vulnerable to theft. Angry and discontented livestock owners who believe the destruction of their animals is unnecessary could put the operators of the system at risk. Unauthorized, graphic photographs or descriptions of the operation could also impact the effort through negative publicity. Most important is that the disease could be spread from the site to other areas. A well-designed security system would control these issues.

The type of security required for carcass disposal operations is obviously not the same as that required for a bank, a nuclear weapon facility, or an infrastructure system; however, an understanding of basic security concepts and design methodology is required for the development of any security system. This basic understanding underlies the design of a system that meets the desired performance objectives. A carcass disposal security system will need to be designed and implemented within a large number of very serious constraints such as time (for design) and cost (of operation). Applying proven physical security design concepts will assure that the best system possible is designed and operated within these real-world constraints.

When designing the carcass disposal security system, clear objectives regarding the actions and outcomes the system is trying to prevent are a necessity. Regardless of the performance goals, all effective security systems must include the elements of detection, assessment, communication, and response.

Three types of adversaries are considered when designing a physical protection system: outsiders, insiders, and outsiders in collusion with insiders. These adversaries can use tactics of force, stealth, or deceit in achieving their goals.

The security system requirements for a carcass disposal system also carry unique characteristics. However, in each case a threat analysis is needed to answer the following questions:

- Who is the threat?
- What are the motivations?
- What are the capabilities?

Before any type of security system can be designed, it is necessary to define the goals of the security system as well as the threats that could disrupt the achievement of these goals.

1.2 – Performance Goals

There will likely be two main components in any large-scale carcass disposal operation. The first component will be the site(s) where processing and disposal operations occur. The second component is the transportation link. In some cases a third component, a regional quarantine boundary, could be considered. For each of these components, a brief description of the action or situation that needs to be prevented provides the basis for the performance goals of an ideal system.

Appropriate security must be provided for these fixed-site operations for all credible threat scenarios. Some unique challenges are presented for mobile operations quickly moving from location to location, but all fixed-site operations share common vulnerabilities that could result in actions that disrupt the controlled disposal of carcasses. At any given fixed disposal site, a range of actions could engage the security system.

This is not to suggest all or even any of these actions *would* occur, only that they *could* occur. It is also important to realize that given the real-world constraints, no security system can be completely effective against all potential actions. In actually designing the system, the designer and analyst must select those actions considered to be the most important and credible and design the system to be most effective against these actions.

The performance goals for the ideal fixed-site security system would be to prevent the following events:

- Interruption of operations.
- Destruction/sabotage of equipment.
- Equipment theft.
- Intimidation of operating personnel.
- Spread of contamination.
- Unauthorized access.

The performance goals for the ideal transportation-link security system would be to prevent the following events:

- Interrupted transfer of people, equipment, and materials (including carcasses).
- Spread of contamination.
- Equipment theft or sabotage.

The performance goal for a regional security system would be to:

- Prevent the unauthorized movement of animals, materials, products, and people across the defined boundary of the region.

Additional performance goals may be determined in collaboration with carcass disposal operations stakeholders.

1.3 – Design Considerations

The design considerations for the ideal security system include (but are not limited to):

- Disposal technology.
- Disposal rationale.
- Prescribed haul routes.
- Disposal system administration.
- Staffing.
- Funding.
- Training.
- Advanced planning and preparation.
- Operational period.
- Geography.

Additional design considerations may be determined in collaboration with carcass disposal operations stakeholders.

1.4 – Threat Analysis

The threat may be very different in cases where there is a natural disaster as opposed to a disease outbreak. In the natural disaster situation the animals will already be dead and there is no question about the need for disposal. In the disease outbreak situation, however, there may be the slaughter of both diseased and healthy, or apparently-healthy, animals. Decisions about the number of animals that need to be destroyed and the geographic area where the animals will be destroyed could become quite controversial.

The threat spectrum for the carcass disposal operations security system design is likely to include two types of threats:

- Malevolent threats (adversaries who intend to produce, create, or otherwise cause unwanted events).
- Nonmalevolent threats (adversaries who unintentionally produce, create, or cause unwanted events).

Carcass disposal operations are unusual in that some of the nonmalevolent adversaries posing a threat to the operations are nonhuman. For example, animals, groundwater, and wind can all spread contamination. The ideal physical security system would prevent these nonhuman adversaries from completing such actions.

Threat analysis for the ideal fixed-site security system would include the following adversaries:

- Intentional malevolent threats, including:
  - Animal owners.
  - Animal rights activists.
  - Site workers/visitors/animals.
  - Unauthorized media.
  - Disgruntled employees.
- Nonmalevolent threats, including:

- Inadvertent intruders
- Curious individuals
- Unintentional insiders
- Animals and other forces of nature

Additional adversaries may be identified in collaboration with carcass disposal operations stakeholders.

1.5 – Security Technology

There are many security technologies available to support the success of designed physical protection systems. Before security technologies can be applied to a carcass disposal operation, the performance goals of the system must be defined, the design considerations must be characterized, and the threat must be analyzed. Only then can a security system be designed to address the needs of the particular problem.

It is possible to expect that sensors, specifically exterior intrusion detection sensors, are likely to be a part of a physical protections system designed to provide security for a carcass disposal operation. For this reason, a technical description of the capabilities of these sensors is provided in Section 7.

1.6 – Recommendations

Several general recommendations for designing an effective security system for carcass disposal operations are provided. The general recommendations include:

- Plan ahead.
- Include local law enforcement in planning.
- Focus on low-cost, rapidly deployable technologies.
- Provide pre-event training.
- Coordinate efforts.
- Understand the legal issues.
- Integrate security plans with biosecurity protocols and procedures

Additional specific requirements and recommendations need to be developed in collaboration with carcass disposal operations stakeholders.

1.7 – Critical Research Needs

In collaboration with owners, operators, and other stakeholders in carcass disposal operations, security designers must develop the performance goals and design constraints for the security system. A thorough threat analysis will be necessary to identify potential adversaries and credible threat scenarios. This information is required before the system can be designed. Design iterations are to be expected, not only because the facility characteristics change (changes in one part of the system may necessitate changes in other parts), but also because the threat analysis may change.

Section 2 – Introduction

Why is there any need to provide security for dead animals? This is probably the first reaction to the suggestion that a security system is needed for carcass disposal operations. At best, the idea of a security system appears odd. However, there are serious issues to be addressed by a security system. Relatively high-value equipment may be used in the operation that would be vulnerable to theft. Angry and discontented livestock owners who believe that the destruction of their animals is unnecessary could put the operators of the system at risk. Unauthorized, graphic photographs of the operation could also impact the effort through negative publicity. Most important is that disease could be spread from the site to other areas. A well-designed security system would control these issues.

The primary purpose of this effort is to identify the main issues associated with physical security of carcass disposal and to describe how an appropriate system might be developed. The effort discusses the expectations for the system, describes how a system might be designed, identifies important design consideration, reviews technology needs, and identifies operation issues.

The following sections describe general principles associated with the design of security systems (Section 3), the performance goals of a security system for carcass disposal operations (Section 4), the design considerations – many of which are currently unknown – for this effort (Section 5), the approach for analyzing the threat (Section 6), and a review of the sensor technologies that can be brought to bear upon the security issues attending carcass disposal (Section 7). Recommendations for the successful performance of this task are presented (Section 8) and, finally, critical research needs (Section 9) are identified.

Section 3 – Physical Security System Concepts and Design Methodology

3.1 – Design Methodology

This section focuses on the general concepts and methodology required for the design of a physical security system. The type of security required for carcass disposal operations is obviously not the same as that required for a bank, a nuclear weapon facility, or an infrastructure system; however, an understanding of basic security concepts and design methodology is required for the development of any security system. This basic understanding underlies the design of a system that meets the desired performance objectives. As discussed below, a carcass disposal security system will need to be designed and implemented within a large number of very serious constraints such as time (for design) and cost (of operation). Applying proven physical security design concepts will assure that the best system possible is designed and operated within these real-world constraints.

Most physical security systems focus on preventing one of two types of actions: theft or sabotage. For example, a bank is primarily concerned with the theft of money. An adversary comes into the bank, takes the money, and must leave the premises with the money to be successful. In a case of sabotage, the adversary needs only to gain access to the facility and complete a destructive act. For example, an activist may wish to halt the production of some product. To be successful, the adversary gains access to the facility or production line in order to destroy or disrupt the production. In an extreme example, the adversary would not even need to gain physical access to the facility but could use standoff weapons such as rocket-propelled grenades to disrupt the operation. Security systems to prevent theft and security systems to prevent sabotage are thus very different. Security systems can also be designed to prevent other types of undesired actions, such as kidnapping, violence against persons, misuse of the facility, or disclosure of information. When designing the carcass disposal security system, clear objectives regarding the actions and outcomes the system is trying to prevent are a necessity. Regardless of the performance goals, all effective security systems must include the elements of detection, assessment, communication, and response.

Three types of adversaries are considered when designing a physical protection system: outsiders, insiders, and outsiders in collusion with insiders.

These adversaries can use tactics of force, stealth, or deceit in achieving their goals. Adversaries can have a variety of different motivations. These motivations may be ideological, economic, or personal. The capabilities of the adversaries can also vary widely. An adversary could be an unarmed individual or a heavily armed paramilitary force. The adversary's level of dedication will also vary. At one

end of the spectrum is the common vandal, who will run away at the first sign of detection; at the other end of the adversary spectrum is the highly dedicated extremist willing to die for a cause.

These factors must be considered in designing the physical protection system. Adversary characteristics are obviously very different when considering the design of a nuclear weapons physical protection system versus a home alarm system. The security system requirements for a carcass disposal system also carry unique characteristics. However, in each case a threat analysis is needed to answer the questions:

- Who is the threat?
- What are the motivations?
- What are the capabilities?

Thus we see that before any type of security system can be designed, it is necessary to define the goals of the security system as well as the threats that could disrupt the achievement of these goals. In the case of carcass disposal, these performance goals and adversaries may be different from those associated with typical physical security systems.

To assure that the system achieves the desired goals, a cyclical design process (see Figure 1) is used. The cycle begins with defining the system requirements followed by a proposed design concept. The effectiveness of the system in meeting the performance goals is then analyzed. The results of the analysis answer the question, "Does the physical protection system meet protection performance goals?" If the system does not meet the stated goals, it must be redesigned. The next design phase attempts to improve weaknesses that have been identified in the system. The design and analysis cycle is closed by analysis of the redesigned system. The cycle is repeated until an effective design is achieved.

In designing the optimal system a wide variety of real-world constraints must be considered. Such constraints may include:

- Budget for design, construction, and operation.
- Time available for design and implementation.
- Expected system lifetime.
- Ability to perform maintenance.
- Power and utility availability.
- Personnel training.
- Operational personnel qualifications (e.g., military professionals, day laborers).

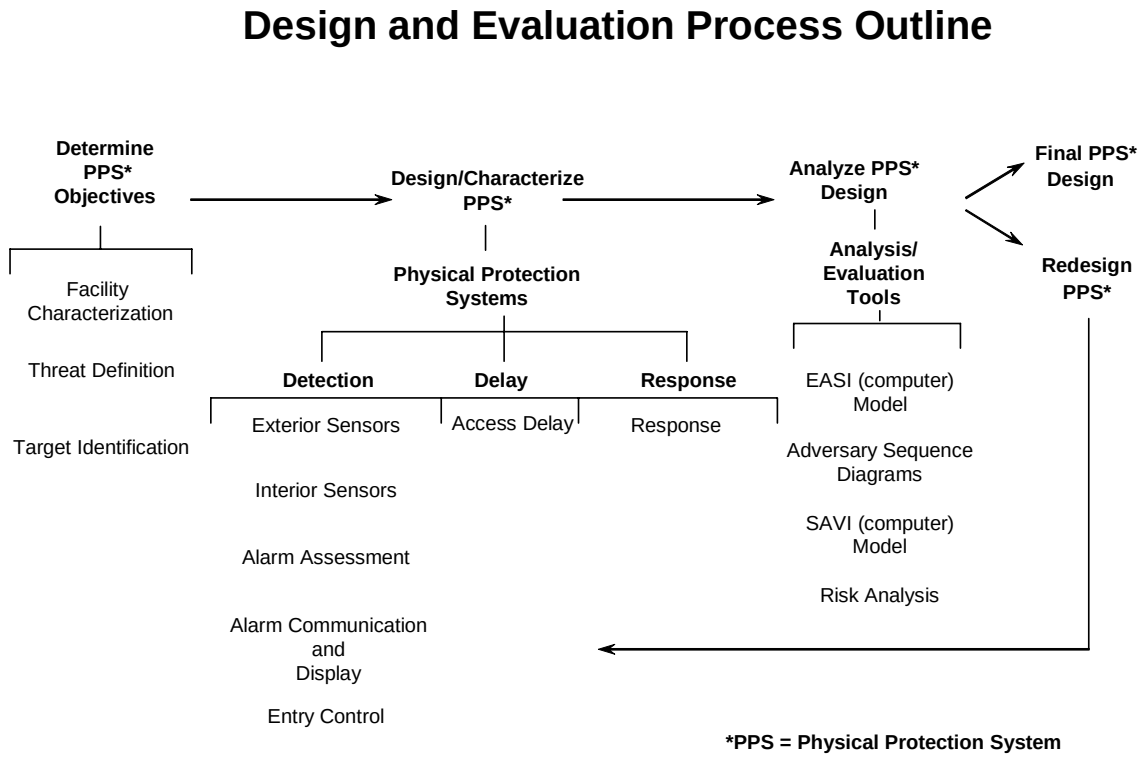


FIGURE 1. The design and evaluation process for physical security systems.

These and other considerations must be factored in when designing the system. Because resources are finite, the design must be optimized to meet the performance goals as successfully as possible within the specified limitations or constraints. Therefore, the iterative design process must factor in all real-world considerations to achieve the optimal design that meets the budget and operational constraints unique to the carcass disposal situation.

A balanced approach that does not allocate all resources to one aspect of the problem while ignoring another is also required. For example, it would be a waste of resources to build a very sturdy, heavily locked gate when it is possible to cut a barbed wire fence and simply drive around the gate. (See Figure 2 for another inappropriate application of security measures.) Once the system is in place, performance metrics are needed to help assess the effectiveness of the system.

In the final analysis, any security system provided for carcass disposal will need to be very low cost, simple to install, easy to maintain, and easy to operate. The reality is that there will be a very limited budget and the system will probably only need to operate for a limited period of time. The following sections focus on understanding the problem and defining the needs and constraints of the system.

FIGURE 2. Clear zone with multiple sensors – part of a robust security system that is not appropriate for the carcass disposal operations problem.

3.2 – Design Application

This section provides a simplified hypothetical example of how the security design process might be applied to a carcass disposal operation.

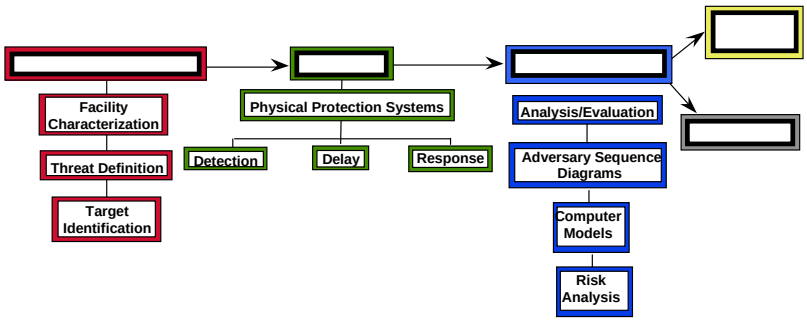
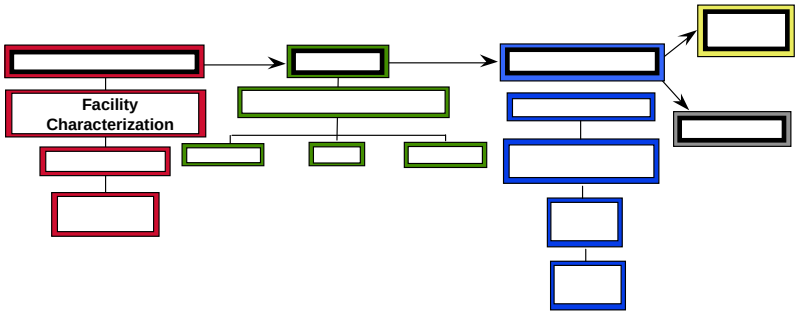
Information needs

Table 1, compiled by Kimberly Asbury of the Intrusion Detection Department at Sandia National Laboratories, provides an outline of the design requirements of a physical protection system in the first column, and credible responses to those information needs are posited in the second column. The second column also contains the preliminary component modeling for a physical protection system to meet the security requirements of the hypothetical carcass disposal site.

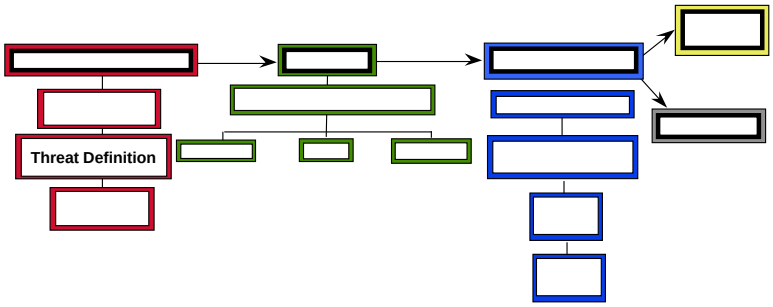
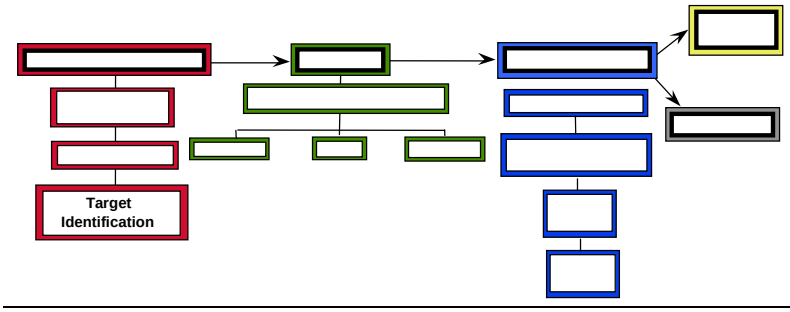
Design options

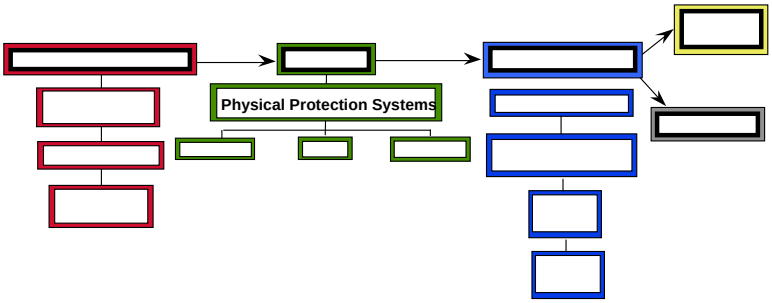
Based on the hypothetical information in the second column of Table 1, a preliminary physical protection system can be designed. Two potential design options were developed as examples. One option is a high-end security system and the other is both less effective and less expensive.

TABLE 1. Model application of the physical security design process for a hypothetical carcass disposal operation.

Information Needs	Site Data (Hypothetical)
	
Facility Characterization (describe the facility)	
	
Physical Conditions	
Topography	Relatively flat even terrain (farming, agricultural lands)
Vegetation	Grasslands and low-density forests
Wildlife	Scavenger animals (coyotes, raccoons, birds, etc.)
Background noise	■ Major highways ■ Railway ■ Small aircraft (crop dusters)
Climate & weather	■ Blizzards, hail, thunderstorms, and tornadoes ■ Temp range from 24oF winters – 90oF summers ■ High humidity
Site boundary	■ Property fencing ■ Naturally occurring boundaries (i.e., river, stream, ditch)
Traffic	■ Heavy equipment (i.e., backhoes, tractors) ■ Semi trucks ■ Trains ■ Personal vehicles
Number, location, and types of buildings in the complex; also, room locations within buildings	Generally low in number, single room, prefabricated, easily mobile ■ Carcass disposal area requirements (will vary depending upon technique used for disposal) ■ Test facility and offices (modular, butler buildings, tents) ■ Ranchers'/farmers' homes, stables, barns, sheds

Access points	■ Pre-existing doors and tent openings ■ Traffic access points into the perimeter
Existing physical protection features	■ Local law enforcement ■ Pre-existing locks on windows and doors of buildings ■ Tent closures
Infrastructure Details	
Heating	Standard design for most buildings
Ventilation & air-conditioning systems	Standard design for most buildings
Communication paths and type (fiber optic, telephone, computer networks, etc.)	■ Cellular ■ Radio
Construction materials of walls and ceilings	■ Fabric walls and roofs for tents ■ Metal 2-x-2 walls and roof for modular units
Power distribution system	■ Generators ■ Hardened lines
Environmentally controlled areas of the facility	Test labs will be environmentally controlled ■ Independent power and ventilation system
Locations of hazardous materials	Type, quantity, and location will depend upon carcass disposal technique ■ Type: Gas (carbon dioxide) and injectibles ■ Fragmentation bullets and captive bolt pistols used in euthanizing the affected animals
Exterior areas	Carcass disposal and storage areas
Facility Goals and Objectives	
Goal	Eradicate and effectively contain the pathogen while minimizing incidents during transport and disposal of carcasses
Processes that support this goal	Enforceable documented regulations (decontamination protocols, safety and security plans)
Operating conditions (work hours, emergency operations, etc.)	Employee schedules, emergency operations, etc.
Types and numbers of employees	■ Shift work ■ Skill set
Support functions	■ Law enforcement ■ Regulatory/federal agencies (USDA, CDC, etc.) ■ Medical ■ Transportation contractors
Facility Policies and Procedures	
Pre-existing documented policies and procedures	
Regulatory Requirements	
Pre-existing requirements imposed by regulatory agencies (e.g., FAA, local law enforcement, emergency response units, etc.)	
Legal Issues	
Safety Considerations	

Effectiveness of current system in normal and abnormal conditions (e.g., fire or flood)	
Threat Definition (describe the adversary)	
	
Type and Motivation	
Malevolent (deliberate acts that result in the spread of contamination or the disruption of the facility)	■ Farmers/ranchers – Owners of the animals to be destroyed could be severely impacted financially ■ Extremists (animal rights activists) – Due to the large number of animals to be destroyed there may be protests ■ Local stakeholders – These individuals may not want contaminated animals being disposed of in their landfills ■ Disgruntled employees – A worker who disagrees with the new work constraints or the act of disposing of such a large number of animals ■ Unauthorized media – Journalists trying to get photographs or a story without undergoing the appropriate approval process
Potential Goals Based Upon Targets	
Tactics, Numbers, and Capabilities	
Malevolent	■ Sabotage, theft ■ Low skills ■ Single to multiple individuals ■ Firearms and explosives ■ Vehicles and heavy equipment ■ Medical supplies
Target Identification (determine & asses the targets)	
	
Undesirable Consequences	■ Spread of the pathogen ■ Interruption of the transfer of people, equipment, and materials (including carcasses) ■ Equipment theft or sabotage
Select Technique for Target Identification	What systems/processes in operation if targeted would result in the undesirable consequences

Identify Targets	■ Carcasses ■ Carcass storage/disposal facilities ■ Test labs ■ Vehicles used to transport materials, people, equipment ■ Equipment/machinery essential to operations
Physical Protection System (design a physical protection system that incorporates detection, delay, and response)	
	
Detection	
P_d Probability of Detection	■ A lower P_d (.70 or higher) can be tolerated due to the realistic threat level being low ■ Adversaries to be detected are humans walking, running, crawling, and climbing; vehicles breaching the perimeter; and scavenger animals
P_a Probability of Alarm (P_d * Probability of Communication)	■ The $P_{a\ will}$ be fairly high due to the response force being onsite local law enforcement
Exterior Sensors	■ The exterior perimeter costs will be the dominant consideration; however, the materials are reusable ■ Entrance – The entrance to the area can be monitored by local law enforcement ■ Outer fence will be an electric net that will keep out scavenger animals as well as reduce nuisance alarms on the inner fence ■ Portable barricades mounted with chain-link fencing and fence-disturbance sensors will be used around the protected area. This will keep out scavenger animals, delay vehicles, and provide delay for alarm assessment
Interior Sensors	Not discussed in this process; however, cost-effective sensors with low nuisance and false alarm rates (such as balanced magnetic switches) should be used
Alarm Assessment	■ Portable halogen lighting ■ Camera images displayed on-site to response personnel ■ A lower resolution black-and-white camera may be used if this video is used for detection and classification rather than prosecution ■ Digital video recorder for storage as well as to provide pre-alarm assessment
Alarm Communication and Display	Local alarm annunciation
Entry Control	Entry control will be performed by law enforcement
Delay	
Delay	■ Jersey barriers at entrance to create a serpentine approach

	to slow down vehicles ■ Jersey barriers around perimeter to stop or slow vehicles ■ Locked gate at entrance ■ Locked gate to the carcass disposal areas and building areas ■ Fences to delay an adversary long enough to ensure good assessment
Response	
Interruption & Neutralization	■ On-site local law enforcement ■ Other response forces used for backup

The following example physical protection designs are based on the hypothetical information presented in Table 1. They are presented for illustrative purposes only.

Design 1: higher-cost option

This perimeter intrusion detection system is capable of detecting a human attempting to cut or climb the inner perimeter fence, protecting against scavenger animals, and protecting against vehicles attempting to ram the perimeter. This system will not protect against birds. Figure 3 shows the layout for Design Option 1.

Design specifications

This example physical protection system was designed for a 1320-foot rectangular perimeter.

Perimeter

Outer fence. This fence is made from low-cost 3.5-foot-high electric netting. The purposes of this fence are to keep out the ground scavenger animals as well as reduce the number of nuisance alarms on the protected areas fence sensor.

Inner fence. This fence is made from off-the-shelf interlocking 32-inch-high barriers with mounted 5-foot-high 9-gauge rolled chain link. Mounted to the fence is a coaxial fence disturbance sensor. The purposes of this fence are to protect the perimeter from vehicle penetration, detect the adversary, and provide the delay required for alarm assessment.

Fence sensor. Coaxial cable sensors provide the desired portability, as maintenance is easier than with fiber disturbance sensors.

Perimeter lighting. Portable halogen work lights mounted on a tripod are recommended to illuminate the area for camera assessment. These are available from home improvement stores at a low cost; another alternative is to rent them for the duration of the operation.

Cameras. One camera per zone is recommended. The cameras should be mounted beneath the lighting to avoid blooming as well as at a slight downward angle to avoid sun glare.

Assessment trailer

This example includes a very simple alarm assessment system that can be used in a field setting.

Alarm control and display. A simple alarm annunciator can be used to detect the relay closures of the sensor. The annunciator can use a horn to alert staff and message LEDs to indicate the different zones of the fence.

Monitor. A low-cost black-and-white monitor with a switcher can be used to view the different cameras and zones.

Cost breakdown for design 1

Costs are presented per-foot using a 1320-foot perimeter, and do not include labor and maintenance.

Item	$/foot
Electric net	$1.06
Barriers	$31.22
Chain link fence (uninstalled)	$2.01
Fence disturbance sensor	$10.00
Assessment (camera, switcher, monitor)	$4.42
Annunciator	$0.12
Lighting	Varies
TOTAL (excluding lighting)	**$48.83**

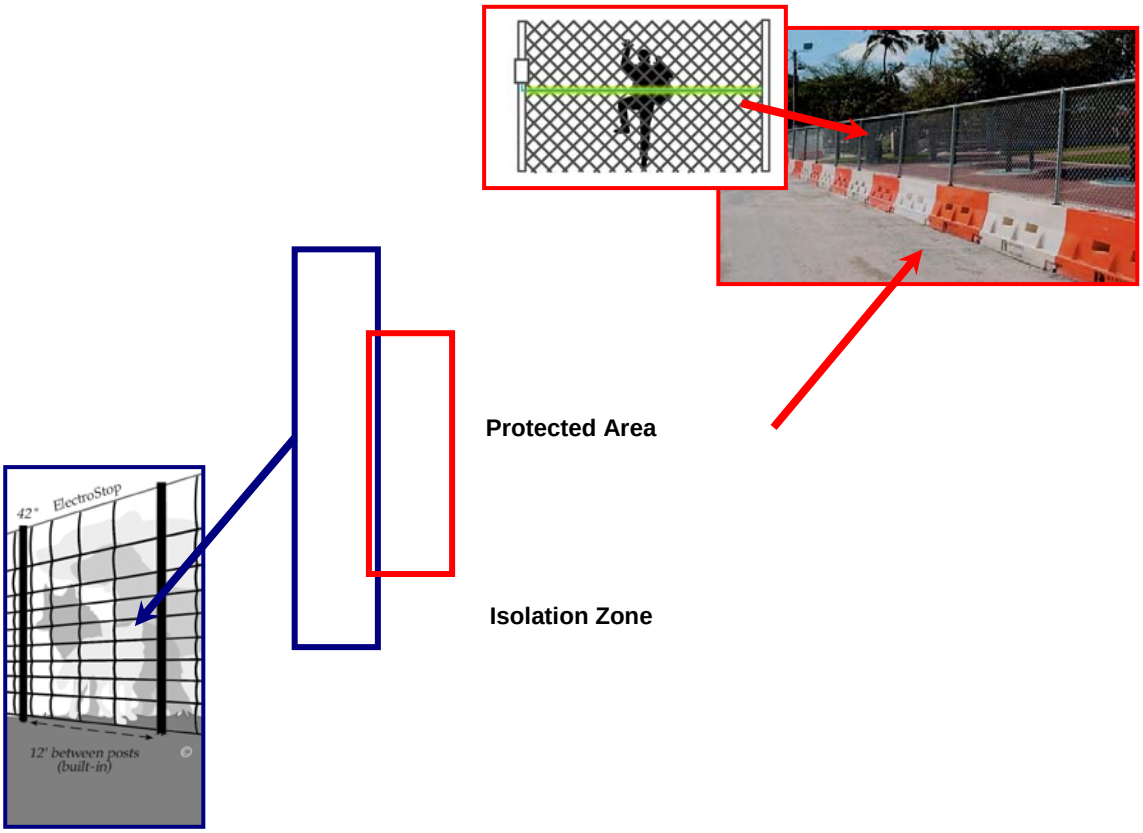


FIGURE 3. Design Option 1 layout diagram.

Design 2: lower-cost option

This perimeter intrusion detection system is capable both of protecting against a person crossing the zone by walking, running, rolling, or crawling and protecting against scavenger animals. This system will not protect against birds. Because it uses exterior passive infrared sensors, this design may have a significantly higher nuisance alarm rate than the higher-cost option. Figure 4 shows the layout for Design Option 2.

Design specifications

This example physical protection system was also designed for a 1320-foot rectangular perimeter.

Perimeter

Perimeter fence. This fence is made from a low-cost 3.5-foot-high electric netting. The purposes of this fence are to keep out the ground scavenger animals as well as reduce the number of nuisance alarms on the protected area passive infrared fence sensors.

This design option does not protect against vehicles and does not offer any delay or detection on the fence line.

Sensors. Exterior passive infrared will be used within the perimeter in order to detect scavenger animals and humans. This type of sensor may have high nuisance alarm rate in some locations.

Perimeter lighting. As in Design 1, portable halogen work lights mounted on a tripod are recommended to illuminate the area for camera assessment. These are available from home improvement stores at a low cost; another alternative is to rent them for the duration of the operation.

Cameras. As in Design 1, one camera per zone is recommended.

Assessment trailer

As in Design 1, this example includes a very simple alarm assessment system that can be used in a field setting.

Alarm control and display. As in Design 1, a simple alarm annunciator can be used to detect the relay closures of the sensor. The annunciator can use a horn to alert staff and message LEDs to indicate the different zones of the fence.

Monitor. As in Design 1, a low-cost black-and-white monitor with a switcher can be used to view the different cameras and zones.

Cost breakdown for design 2

Costs are presented per-foot using a 1320-foot perimeter.

Item	$/foot
Electric net	$1.06
Exterior passive infrared sensor	$31.22
Assessment (camera, switcher, monitor)	$4.42
Annunciator	$0.12
Lighting	Varies
TOTAL (excluding lighting)	**$10.85**

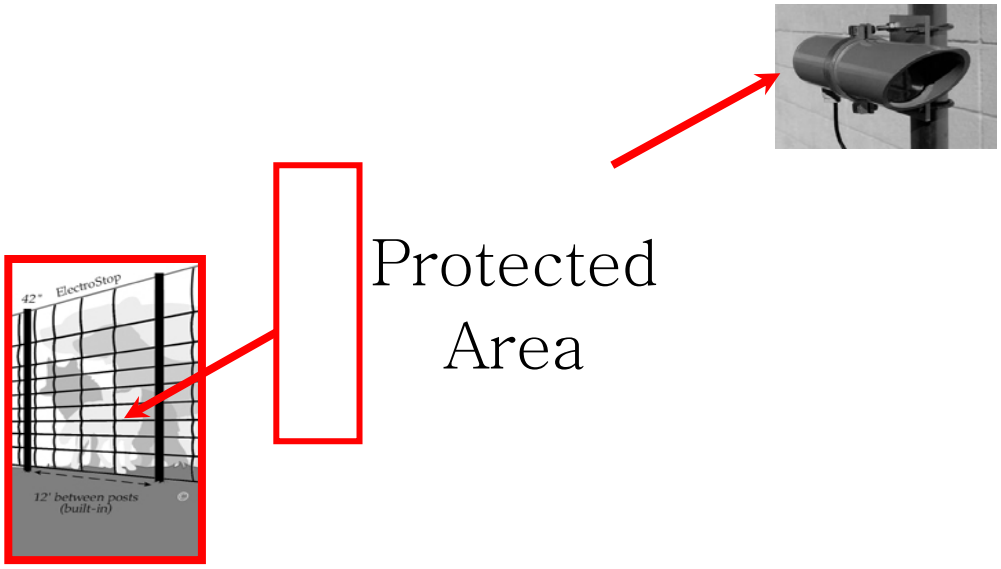


FIGURE 4. Design Option 2 layout diagram.

Section 4 – Performance Goals

This analysis assumes that large numbers of animals are involved and that the processing operation will require weeks or even months. Small-scale disposal activities, such as those associated with normal production losses, are not considered here. These types of operations do not require any formal review of security beyond what is normally provided for farm or processing operations. Similarly small-scale disposal operations necessitated by a local problem (such as a fire or small flood) do not need security planning other than that required as part of normal operational practices. In these cases, normal industrial security practices, such as locking or disabling heavy equipment, is probably adequate.

However, large-scale carcass disposal, with the possibility of pathogen movement, the use of large amounts of heavy equipment, and the potential to generate anger and discontent over decisions made by policy makers, creates a unique security situation.

There will most likely be two main components in any large-scale carcass disposal operation. The first component will be the site(s) where processing and disposal operations occur. The second component is the transportation link. In some cases a third component, a regional quarantine boundary, could be considered. For each of these components, a brief description of the action or situation that needs to be prevented provides the basis for the performance goals of an ideal system.

4.1 – Fixed-Site Processing and Disposal Operations

Processing (grinding, chopping, etc.) and disposal could occur at a regional location where live animals are brought for slaughter, processing, and disposal, or where dead animals are brought for processing and disposal. It is possible that slaughter and some preprocessing will be performed at multiple locations and the carcasses then transported to the regional center. It is even possible that mobile systems will be utilized. In this case, operations would be established for a short period of time at one location (such as a feedlot) and then moved to another location.

In all these scenarios, appropriate security must be provided for these fixed-site operations. Some unique challenges are presented for mobile operations that are quickly moved from location to location, but all fixed-site operations share common vulnerabilities that could result in actions that disrupt the controlled disposal of carcasses. At any given fixed disposal site, a range of actions could be encountered by the system. Each of these actions is discussed below.

This is not to suggest all or even any of these actions *would* occur, only that they *could* occur. It is also important to realize that given the real-world constraints, no security system can be completely effective against all potential actions. In actually designing the system, the designer and analyst must select those actions considered to be the most important and credible and design the system to be most effective against these actions.

Interruption of operations

A goal of some adversaries may be to interrupt operations. Individual or group motivations could range from objections to the destruction of animals to environmental concerns about the disposal process to opposition to the proximity of the operations to individual's properties. Some examples of how the operations could be interrupted are described in the following paragraphs.

Site blockade

Adversaries could attempt to block access to the sites where disposal operations are occurring. This could take the form of individuals blocking roadways, vehicles and equipment blocking site entrances, or even picket lines. In these situations, trucks carrying animals, operational personnel, or support equipment could be prevented from entering the site.

Prevention of access to animals

Adversaries may inhibit access to their farms, facilities, and operations to prevent the removal of animals or prohibit their destruction on site. These actions could delay or prevent the destruction of animals.

Disruption of support utilities

Adversaries cutting the power lines could interrupt disposal operations reliant on off-site power. Similarly, gas and water services supplied through off-site pipelines could be interrupted.

Intimidation of workers

Workers could fail to report to work if they feel threatened in the local community.

Destruction or sabotage of equipment

Most disposal options require the use of heavy equipment. Much of this heavy equipment could be easily sabotaged. Animal-handling equipment could include loaders, backhoes, tractors, and trucks. Disposal equipment may include incinerators, grinders, and composting materials. There are three obvious ways such equipment could be sabotaged:

- Mechanical sabotage.

  Sabotage can include actions typically thought of as vandalism, such as breaking critical mechanical components with crowbars or baseball bats.

- Fire.

  Arson could be used to destroy individual pieces of equipment or entire carcass disposal facilities, such as rendering plants.

- Fuel contamination.

  Equipment fuel tanks, on-site storage tanks, or even fuel supply trucks could all be contaminated to prevent operation of the equipment.

Equipment theft

This is one of the most likely security concerns at a carcass disposal operation due to the relatively high-value heavy equipment used at the site. These pieces of equipment are attractive because of their value and versatility of use. Equipment theft is the most common industrial concern.

Intimidation of operating personnel

Because of anger about the destruction of apparently healthy animals, there could be threats of violence or actual assaults against operating personnel.

Contamination spread

Strictly speaking, industrial hygiene or biosecurity, defined as the precautions taken to contain pathogens, may not be considered a security issue. However, the goals of biosecurity and physical security are so closely aligned that the distinction seems artificial (although some protection measures are implemented solely for biosecurity or physical security). Any designed security system must be required to prevent the spread of pathogens from the site. This goal is relevant whether animals are being destroyed because of a disease outbreak or because of a natural disaster. In the case of a natural disaster, rotting carcasses will harbor diseases that require containment. An unusual aspect of preventing the removal of pathogens from the site to be considered is that the threat is not just realized through human adversaries. Pathogens could be removed from the site via a number of different pathways: air/wind, animals (birds, mammals, insects), groundwater, equipment movement, or human activity (workers, visitors, intruders).

Unauthorized access

Individuals may try to enter the site because of malicious intent, curiosity, or even by accident. Because the site will contain heavy equipment and perhaps other dangerous processing machinery, the site is hazardous for visitors. Thus the ideal security system will prevent unauthorized access to the site for innocent visitors as well as malevolent adversaries.

The performance goals for the ideal fixed-site security system would be to prevent the following events:

- Interruption of operations.
- Destruction/sabotage of equipment.
- Equipment theft.
- Intimidation of operating personnel.
- Spread of contamination.
- Unauthorized access.

Additional performance goals may be determined in collaboration with carcass disposal operations stakeholders.

4.2 – Transportation Links

In any sizeable carcass disposal operation, transportation links will be a part of the process. At a minimum, there will be delivery of equipment and

consumables to the site. It is possible that live or dead animals will be collected throughout an area and then transported to the disposal site. At any given fixed disposal site, a range of actions encountered by the transportation link could disrupt controlled carcass disposal operations.

Interrupted transfer of people, equipment, or material

Adversaries could block transportation routes to prevent delivery of disposal operations supplies, such as fuel or equipment, or drivers could be prevented access to animals to be removed.

Spread of contamination

Vehicles may be moving in and out of contaminated areas. Because of this there may be an unintentional spread of contamination from the disposal site or the vehicles. In addition, live or dead animals may be transported which could also cause the spread of contamination.

Equipment theft or sabotage

As with fixed-site operations, equipment could be stolen or sabotaged at the transportation links.

The performance goals for the ideal transportation-link security system would be to prevent the following events:

- Interrupted transfer of people, equipment, and materials (including carcasses).
- Spread of contamination.
- Equipment theft or sabotage.

Additional performance goals may be determined in collaboration with carcass disposal operations stakeholders.

4.3 – Regional Boundary Security

In the case of the outbreak of a disease, officials may make the decision to quarantine an entire area or region. This quarantine could require the cessation of movement of certain types of animals. It could also restrict the shipment of certain products or, in some cases, even individuals, such as agricultural workers. Although issues associated with regional security are beyond the scope of this study, the main issues should be considered, as there may be an impact on the design of the physical protection system for carcass disposal. It is imperative that plans are in place and agencies have coordinated plans prior to an outbreak.

Large resources are required for regional boundary security systems, which will undoubtedly be beyond the capabilities of local jurisdictions. State or even federal support, such as the National Guard, will be required to support the manpower requirements of these operations. These operations could require stopping and searching large numbers of vehicles. The transport of animals, individuals, equipment, and products would all be affected. All modes of travel (roads, rail, river or coast, air) into and out of the area would be monitored.

As the number of checkpoints increases, personnel requirements rapidly become unmanageable. To help minimize the resource requirements, natural choke points should be identified for the region. For example, inspections could be set up at a few river bridges rather than along all roads. In addition, there may be the need to perform some type of patrols or spot-checking along the quarantine boundary.

Training will be required for the individuals involved in these operations. Legal issues associated with searches must be carefully addressed.

The performance goal for a regional security system would be to prevent the unauthorized movement of animals, materials, products, and people across the defined boundary of the region.

Additional performance goals may be determined in collaboration with carcass disposal operations stakeholders.

Section 5 – Design Considerations

This section briefly describes some elements that affect the design and operation of the security system.

5.1 – Disposal Technology

The type of technology chosen for the carcass disposal will have tremendous implications for the design of the security system. For example, if the entire operation is contained in enclosed buildings the security system can focus on the doors and other penetrations of the building. However, if equipment and operations are mobile and moved from farm to farm, then portable, rapidly deployable equipment will be required.

5.2 – Disposal Rationale

If disposal operations are occurring because of an outbreak of a contagious pathogen such as foot-and-mouth disease, the security system will need to consider biosecurity practices and assure the security system is complementary. If, however, disposal is occurring because of a noninfectious agent such as bovine spongiform encephalitis (BSE), security may focus more on the protection of the assets used in the disposal operation. In the BSE case, strict security and biosecurity measures would not be required for the transport of live animals or carcasses.

5.3 – Prescribed Haul Routes

There may be reluctance in a community to have trucks carrying dead animals or potentially infected animals through certain areas or on certain roads. The local population may have health concerns or there may be concern about transportation adjacent to areas where animals have not been affected by a disease outbreak. There may even be concerns about tourism, so that transportation is prohibited through tourist areas. Prescribed haul routes have been required in previous carcass disposal situations. Because of concerns about deviations, the local population may request some type of monitoring and enforcement of the agreed-upon haul routes.

5.4 – Disposal System Administration

Depending upon the reason for the disposal operation and its size, the entire operation could be administered by local, state, or even federal entities. These different levels of administration will have direct implications for how a security system can be designed and implemented. If the disposal operation is managed at the local level using local resources, funding and flexibility in system design may be very limited. In this case, existing law enforcement resources may provide security for the site. As administration goes to higher levels, more resources and funding may be brought to bear on the problem, thus allowing higher utilization of technologies.

5.5 – Staffing

Local law enforcement professionals, contracted security professionals, or the National Guard could operate the security system. Each of these operators will offer different design implications. Decisions about staffing will affect how the security system is designed. If the National Guard provides continuous patrols of a perimeter, the need for technological solutions will likely be reduced.

5.6 – Funding

System design and operation will always be limited by funding. In considering the design of the system, however, economic trade-offs will need to be made. For example, utilizing technology can sometimes offset manpower costs.

5.7 – Training

The possibility of training individuals in the use of the security system before an incident occurs versus training only after the disposal operations have begun should be considered. If training can only occur after the onset of an incident, a technically and procedurally simple security system is required.

5.8 – Advanced Planning and Preparation

If relevant agencies are able to plan for potential carcass disposal events, there will be more opportunities to control the costs associated with security. If, however, design only occurs at the inception of an event, high-cost, manpower-intensive solutions will probably be implemented. Advanced planning can lead to agreements on who will be providing security and how it will be implemented. There may even be opportunities to purchase needed technologies prior to an event or to identify resources already available in the area that could be applied. If planning occurs before an event, agreements can be developed between jurisdictions for sharing or loaning equipment.

5.9 – Operational Period

This analysis assumes that the carcass disposal operations will be occurring for at least a few weeks. If the disposal operation is very short-term, there will be little motivation to invest in security technologies. However, as the length of time increases for the disposal operation, there is increasing motivation to decrease labor costs through the application of technology. It should also be noted that the nature of the threat might change over time.

5.10 – Geography

Natural barriers can play a role in the security system. As an example, an open-pit mine was used as the base of carcass disposal operations in North Carolina. The vertical sides of the mine provided a natural deterrent for human intrusion into the site. Other geographic features can either assist or impede the security system. Flat treeless areas provide a good location for ease of assessment. Heavily forested areas make patrol and monitoring of a perimeter difficult.

To identify the design considerations applicable to a specific carcass disposal operation, the characteristics of the operation must be determined. The design considerations for the ideal security system include (but are not limited to):

- Disposal technology.
- Disposal rationale.
- Prescribed haul routes.
- Disposal system administration.
- Staffing.
- Funding.
- Training.
- Advanced planning and preparation.
- Operational period.
- Geography.

Additional design considerations may be determined in collaboration with carcass disposal operations stakeholders.

Section 6 – Threat Analysis

Carcass disposal security systems will probably not be facing a large paramilitary force armed with automatic weapons and explosives. The threat will be very different in cases where there is a natural disaster as opposed to a disease outbreak. In the natural disaster situation, the animals will already be

dead and there is no question about the need for disposal. In the disease outbreak situation, however, the slaughter of diseased and healthy or apparently healthy animals may be required. Decisions about the number of animals to be destroyed and the geographic limits of the area in which animals will be destroyed could become quite controversial. There are several categories of people who may be impacted by the carcass disposal operation. The following discussion illustrates the spectrum of threats that the security system could be expected to address.

6.1 – Intentional Malevolent Threats

Animal owners

Individuals could be severely impacted economically if their animals are destroyed. Some breeding animals could be quite valuable. These individuals could potentially be armed and may not appear rational.

It should be noted that in previous animal destruction situations there have been concerns regarding farmers "cheating" the system. Farmers will bring in animals for destruction and receive compensation for their destruction. The farmers then instead of taking the animals to be destroyed will surreptitiously remove the animals and then bring them back again and receive compensation a second time.

Animal rights activists

Because thousands or even millions of animals may be destroyed, there may be some form of protest from animal rights activists.

Local stakeholders

People may not want thousands of dead animals disposed of in their local landfills or processed in their backyards.

Unauthorized media

Journalists trying to obtain information or photographs of the operation without proper approval to be on the site create a nuisance problem, at the least.

Disgruntled employees

As with any work environment, there is a possibility for individual workers to be a threat. Adversaries who represent malevolent threats may engage in such activities as:

- Civil disobedience, such as protests or blockade.
- Vandalism.
- Verbal or physical intimidation of workers.
- Armed or unarmed assault against workers.
- Theft.

Such activities can result in the spread of contamination or the disruption of operations.

6.2 – Unintentional Nonmalevolent Threats

Human and animal movements can result in the inadvertent transfer of pathogens. The activities of these unwitting adversaries can result in the spread of contamination or the disruption of operations similar to the impact of the intentional activities of the malevolent adversary.

Inadvertent intruders

Disposal sites could be quite large. It is possible that individuals could unknowingly enter the site while hiking or hunting, for example.

Curious individuals

In previous carcass disposal operations, curious onlookers have been a significant issue. These onlookers have lined the road to the disposal site. This can potentially impede access and create a dangerous situation.

Unintentional insider (site workers/visitors)

Site workers or approved visitors may accidentally remove contamination from the site by not following decontamination protocols.

Animals

It may be considered the role of the security system to help prevent animals from entering and exiting the site and transporting pathogens off site (Figure 5).

FIGURE 5. Prairie dogs are a threat to spread contamination.

Section 7 – Security Technology

There are many security technologies available to support the success of designed physical protection systems. Before security technologies can be applied to a carcass disposal operation, the performance goals of the system must be defined, the design considerations must be characterized, and the threat must be analyzed. Only then can a security system be designed to address the needs of the particular problem.

It is possible to expect that sensors, specifically exterior intrusion detection sensors, are likely to be a part of a physical protections system designed to provide security for a carcass disposal operation. For this reason, a technical description of the capabilities of these sensors is provided below.

7.1 – Exterior Intrusion Detection Sensors

The integration of individual sensors into a perimeter sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the perimeter system with a balanced and integrated physical protection system. Sensor performance is described by the following characteristics: probability of detection (P_D), nuisance alarm rate (NAR), and vulnerability to defeat.

The methods of classification of exterior sensors include passive or active, covert or visible, line of sight or terrain-following, volumetric or line detection, and application (buried-line, fence-associated, or freestanding). This section presents several examples of sensors in each application category. An effective perimeter sensor system

provides a continuous line of detection using multiple lines of complementary sensors located in an isolated clear zone. Topography, vegetation, wildlife, background noise, climate, weather, soil conditions, and pavement all affect the performance of exterior sensors. The designer of the perimeter sensor system must also consider its interaction with the video assessment system and the access delay system.

Introduction

Overview

Intrusion detection systems consist of exterior and interior intrusion sensors, video alarm assessment, entry control, and alarm communication systems all working together. Exterior sensors are those used in an outdoor environment, and interior sensors are those used inside buildings.

Intrusion detection definition

Intrusion detection is defined as the detection of a person or vehicle attempting to gain unauthorized entry into an area that is being protected. The intrusion detection boundary is ideally a sphere enclosing the item being protected so that all intrusions, whether by surface, air, underwater, or underground, are detected. The development of intrusion detection technology has emphasized detection on or slightly above the ground surface with increasing emphasis being placed on airborne intrusion. Ground-level perimeter intrusion detection systems are relevant to detection systems for carcass disposal.

Performance characteristics

Fundamentals of intrusion sensor performance

Intrusion sensor performance is described by three fundamental characteristics:

- Probability of detection (P_D).
- Nuisance alarm rate (NAR).
- Vulnerability to defeat.

An understanding of these characteristics is essential for designing and operating an effective intrusion sensor system.

Probability of detection (P_D)

Ideal sensors have 100% success. For the ideal sensor, the probability of detection (P_D) of an intrusion is one (1.0). That is, it has a 100% P_D. However, no sensor is ideal, and the P_D is, therefore, always less than 1.0. The way that P_D is calculated does not allow a P_D of 1. Even with thousands of tests, the P_D only approaches 1. The P_D depends primarily upon:

- Target to be detected.
- Sensor hardware design.
- Installation conditions.
- Sensitivity adjustment.
- Weather conditions.
- Condition of the equipment.

All of the above conditions can vary; thus despite the claims of some sensor manufacturers, a specific P_D cannot be assigned to one component or set of sensor hardware. For a P_D value to be meaningful, the conditions of the test must be carefully explained.

Nuisance alarm rate (NAR)

Description. A nuisance alarm is any alarm that is not caused by an intrusion. In an ideal sensor system, the NAR would be zero (0.0). However, in the real world, all sensors interact with their environment and they cannot discriminate between intrusions and other events in their detection zone. Alarm assessment systems are needed because not all sensor alarms are caused by intrusions.

Sources of nuisance alarms. Usually nuisance alarms are further classified by source. Both natural and industrial environments can cause nuisance alarms. Common sources of natural nuisance alarms are vegetation (trees and weeds), wildlife (animals and birds), and weather conditions (wind, rain, snow, fog, lightning). Industrial sources of noise include ground vibration, debris moved by wind, and electromagnetic interference.

False alarms. False alarms are those nuisance alarms generated by the equipment itself, whether by poor design, inadequate maintenance, or component failure. Different types of intrusion sensors have different sensitivities to these nuisance or false alarm sources, as is discussed in detail later.

Vulnerability to defeat

Sensor defeat methods. An ideal sensor could not be defeated; however, all existing sensors can be defeated by a knowledgeable adversary with the proper tools and enough time. The objective of the physical protection system designer is to make the system very difficult to defeat. The two general ways to defeat the system are:

- Bypass. Because all intrusion sensors have a finite detection zone, any sensor can be defeated by going around its detection volume.
- Spoof. Spoofing is any technique that allows the target to pass through the sensor's normal detection zone without generating an alarm. Different types of sensors and sensor models have different vulnerabilities to defeat.

Sensor classification

In this discussion, five methods of classification are used:

- Passive or active.
- Covert or visible.
- Line of sight or terrain-following.
- Volumetric or line detection.
- Application.

Passive or active

Passive sensors detect energy. Passive sensors detect some type of energy that is emitted by the target of interest or detect the change of some natural field of energy caused by the target. Examples of the former are mechanical energy from a human walking on the soil or climbing on a fence. An example of the latter is a change in the local magnetic field caused by the presence of a metal.

Active sensors transmit energy. Active sensors transmit some type of energy and detect a change in the received energy created by the presence or motion of the target.

Advantages and disadvantages. The distinction of passive or active has a practical importance. The presence or location of a passive sensor is more difficult to determine than that of an active sensor, which puts the intruder at a disadvantage. Active sensors may be less affected by environmental conditions than passive sensors, because they are transmitting signals selected to be compatible with those conditions. Because of this, an active sensor typically may have fewer nuisance alarms than a passive sensor in the same environment.

Covert or visible

Comparison of sensor types. *Covert sensors* are hidden from view, such as buried in the ground. Covert sensors may have signal emanations that can be detected using electronic equipment. Covert sensors are more difficult for an intruder to detect and locate (than visible sensors), and thus they can be more effective. Also, they do not disturb the appearance of the environment.

Visible sensors are in plain view of an intruder, such as attached to a fence or mounted on another support structure. Visible sensors may deter the intruder from acting. They are typically simpler to install and easier to repair than covert ones.

Line of sight or terrain-following

Line of sight sensors require specific site preparation. Line of sight sensors perform acceptably only when installed with a clear line of sight in the detection space. This usually means a clear line of sight between the transmitter and receiver for active sensors. These sensors normally require a flat ground surface, or at least a clear line of sight from each point on the ground surface to both the transmitter and receiver. The use of line of sight sensors on sites without a flat terrain requires expensive site preparation to achieve acceptable performance.

Terrain-following sensors. Terrain-following sensors detect equally well on flat and irregular terrain. The

transducer elements and the radiated field follow the terrain and result in uniform detection throughout the detection zone. Some terrain-following sensors may require some leveling between fence posts to maintain a high P_D.

Volumetric or line detection

Factors that affect volumetric detection. Volumetric sensors detect intrusion in a volume of space. An alarm is generated when an intruder enters the detection volume. The detection volume is generally not visible and is difficult for the intruder to precisely identify. The detection volume characteristics are based upon frequency, antenna properties, and other factors. Other factors, such as cable spacing, mounting height, sensitivity, and alignment, can make the exact detection volume difficult for an intruder to determine.

Line detection detects at a specific point. Line detection sensors detect along a line. For example, sensors that detect fence motion are mounted directly on the fence. The fence becomes a line of detection, since an intruder will not be detected while approaching the fence; detection occurs only if the intruder moves the fence fabric where the sensor is attached. The detection zone of a line detection sensor is usually easy to identify.

Application

Modes of sensors: buried line, fence, and freestanding. In this classification method, the sensors are grouped by mode of application in the physical detection space. These modes are:

- Buried line. The sensor is in the form of a line buried in the ground.
- Fence-associated. The sensor either is mounted on a fence or forms a sensor fence.
- Freestanding. The sensor is being neither buried nor associated with a fence, but mounted on a support in free space.

Sensor technology

In this discussion, sensors are grouped by their modes of application. Table 2 summarizes exterior intrusion sensor technologies according to the different sensor classification schemes.

TABLE 2. Types of perimeter sensors.

	Passive (P) or Active (A) Detection	Covert (C) or Visible (V)	Line of Sight (LOS) or Terrain-Following (TF)	Volumetric (VOL) or Line (L)
Buried Line				
Seismic Pressure	P	C	TF	L
Magnetic Field	P	C	TF	VOL
Ported Coax	A	C	TF	VOL
Fiber-Optic Cables	P	C	TF	L
Fence-Associated				
Fence Disturbance	P	V	TF	L
Sensor Fence	P	V	TF	L
Electric Field	A	V	TF	VOL
Freestanding				
Active Infrared	A	V	LOS	VOL
Passive Infrared	P	V	LOS	VOL
Bistatic Microwave	A	V	LOS	VOL
Dual Technology	A	V	LOS	VOL
Video Motion	P	C	LOS	VOL

Buried-line sensors

Types of buried line sensors

Types of buried-line sensors that depend on different sensing phenomena include:

- Pressure or seismic sensors.
- Magnetic field sensors.
- Ported coaxial cable sensor.
- Fiber-optic sensors.

Pressure or seismic

Description and applications. Pressure or seismic sensors are passive, covert, terrain-following sensors that are buried in the ground. They respond to disturbances of the soil caused by an intruder walking, running, jumping, or crawling on the ground. Pressure sensors are generally sensitive to lower frequency pressure waves in the soil, and seismic sensors are sensitive to higher frequency vibration of the soil.

Pressure sensor technology. A typical pressure sensor consists of a reinforced hose filled with a pressurized liquid and connected to a pressure transducer. A balanced pressure system consists of two such hoses connected to a transducer to permit differential sensing and to reduce nuisance alarms from seismic sources located far away.

Seismic sensor technology. A typical seismic sensor consists of a string of geophones. A geophone consists of a conducting coil and a permanent magnet. Either the coil or the magnet is fixed in position, and the other is free to vibrate during a seismic disturbance; in both cases an electrical current is generated in the coil. Alternating the polarity of the coils in the geophone string can reduce far-field effects in seismic sensors.

Sensitivity and burial depth. The sensitivity of this type of sensor is very dependent on the type of soil in which it is buried. The best burial depth is also dependent on the soil. The trade-off is high P_D with narrow detection width at a shallow depth versus lower P_D with wider detection width at a greater depth. A test conducted on site with short test sections of the sensor buried at different depths is recommended to determine the optimum depth. A typical detection width for walking intruders is in the range of 1– 2 m.

Effects of winter weather. Pressure and seismic sensors tend to lose sensitivity in frozen soil. Thus, at sites where the soil freezes in winter, either reduced winter sensitivity must be accepted, or a semiannual adjustment to pressure and seismic sensors must be made to obtain equivalent sensitivity throughout the year.

Nuisance alarms for seismic sensors. Many sources of seismic noise may affect these sensors and cause nuisance alarms. The primary natural source of nuisance alarms is wind energy that is transmitted into the ground by fences, poles, and trees. Seismic sources made by man include vehicular traffic (cars, trucks, trains) and heavy industrial machinery.

Defeat methods. Because these sensors are passive and buried, movement above the ground is not detected. If the location of the buried-line sensor is known, an adversary may defeat this sensor by forming a low bridge over the transducer line.

Magnetic field

Detect vehicles and intruders with metal weapons. Magnetic field sensors are passive, covert, terrain-following sensors that are buried in the ground. They respond to a change in the local magnetic field caused by the movement of nearby metallic material. Thus magnetic field sensors are effective for detecting vehicles or intruders with weapons.

Technology description, nuisance alarms, defeat method. This type of sensor consists of a series of wire loops or coils buried in the ground. Movement of metallic material near the loop or coil changes the local magnetic field and induces a current. Magnetic field sensors can be susceptible to local electromagnetic disturbances such as lightning. Intruders who are not wearing or carrying any metal may be able to defeat this type of sensor.

Ported coaxial cables

Description. Ported coaxial cable sensors are active, covert, terrain-following sensors that are buried in the ground. They are also known as leaky coax or radiating cable sensors. This type of sensor responds to motion of a material with a high

dielectric constant or high conductivity near the cables. These materials include both the human body and metal vehicles.

Technology. The name of this sensor is derived from the construction of the transducer cable. The outer conductor of this coaxial cable does not provide complete shielding for the center conductor; thus some of the radiated signal leaks through the ports of the outer conductor. The detection volume of ported coax sensors extends significantly above the ground: about 0.5 to 1.0 m above the surface and about 1 to 2 m wider than the cable separation. The sensitivity of this type of sensor in frozen soil actually increases slightly relative to thawed conditions. This is because some of the field energy is absorbed by conductive soil, and the conductivity of frozen ground is less than that of thawed ground.

Installation. Some ported coaxial cables use a foil shield with a slot instead of actual ports. A semiconductive inner jacket allows the combination of the two cables into a single outer jacket. This allows the sensor to be installed more easily because only a single trench is required and cable spacing is no longer an issue. The disadvantage is that the detection volume is slightly smaller than for a dual cable system with wider cable spacing.

Nuisance alarms. Metal or water in the ported coax detection zone can cause two types of sensor problems. Moving metal objects and moving water are large targets for ported coax sensors and, thus, are a major potential source of nuisance alarms. Both flowing water and standing water contribute to this problem. The second problem is that fixed metal objects and standing water distort the radiated field, possibly to the extent of creating insensitive areas with no detection. Nearby metal objects or utility lines should be excluded from the detection volume. This includes above ground fences and poles and underground water lines and electrical cables.

Fiber-optic cables

Description. Optical fibers are long, hair-like strands of transparent glass or plastic. Fiber optics is the class of optical technology that uses these transparent fibers to guide light from one end to the other. A fiber-optic cable consists of an inner core of pure material and a cladding material that is usually the same material as the core with additional "doping" material added. Because the cladding is designed to have a different refraction of light, the light ray is bent back towards the center of the core. Thus the fiber becomes a "light pipe" (Figure 6). A fiber can either be multi-mode or single-mode depending upon the thickness of the core of the fiber. Single-mode fibers are so thin that only a single light path is possible through the core.

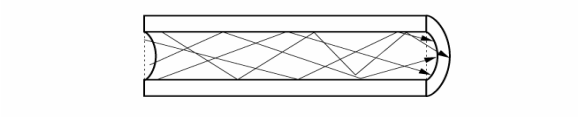


FIGURE 6. Optical fiber guides light.

Fiber-optic cable technology. A fiber optic cable does not have to be straight because the characteristics of the fiber allow light to remain in the core. The light diffraction (speckle) pattern and the light intensity at the end of the multi-mode fiber is a function of the shape of the fiber over its entire length. Even the slightest change in the shape of the fiber can be sensed using sophisticated sensors and computer signal processing at the far end (100 meters or more). A single mode fiber can also be used as a sensor by splitting the light source and sending it both directions around a loop. If the fiber is disturbed, the two light sources come back in a different phase. The change in phasing relates to the amount of disturbance. Thus a single strand of fiber optic cable, buried in the ground at the depth of a few centimeters, can very effectively give an alarm when an intruder steps on the ground above the fiber. To ensure that an intruder steps above the fiber, it is usually woven into a grid and buried just beneath the surface. Fiber-optic cables are also commonly used as fence disturbance sensors.

Fence-associated sensors

General types

Three types of intrusion sensors either mount on or attach to a fence or form a fence using the transducer material:

- Fence disturbance sensors.
- Sensor fences.
- Electric field or capacitance sensors.

Fence disturbance sensors

Description. Fence disturbance sensors are passive, visible, terrain-following sensors designed for installation on a security fence, typically constructed with chain-link mesh. These sensors are considered terrain-following because the chain-link mesh is supported every 3 m with a galvanized steel post, thus the fence itself is terrain-following.

Mechanical disturbances. Fence disturbance sensors respond to mechanical disturbances of the fence. They are intended to detect primarily an intruder who climbs on or cuts through the fence fabric. Several kinds of transducers are used to detect the movement or vibration of the fence. These include switches, electromechanical transducers, fiber-optic cables, and strain-sensitive cables.

Nuisance alarms. Fence disturbance sensors respond to all mechanical disturbances of the fence, not just intruders. Common disturbances include strong winds, debris blown by wind, rain driven by wind, hail, and seismic activity from nearby traffic and machinery. Good fence construction, specifically rigid fence posts and tight fence fabric, is important to minimize nuisance alarms.

Defeat methods. Digging under the fence or bridging over the fence without touching the fence can defeat fence disturbance sensors. Digging can be deterred by putting concrete under the fence. The bottom edge of the fabric can also be placed in the concrete, although this may be undesirable for corrosive environments where the fabric must be replaced frequently.

Sensor fences

Description. Sensor fences are passive, visible, terrain-following sensors that make use of the transducer elements to form a fence itself. These sensor fences are designed primarily to detect climbing or cutting on the fence. Sensor fences tend to be much less susceptible to nuisance alarms than fence disturbance sensors. However, because sensor fences also have a plane of detection that is well defined, they are vulnerable to the same defeat methods as fence disturbance sensors.

Taut wire sensor fences. Taut wire sensor fences consist of many parallel, horizontal wires with high tensile strength that are connected under tension to transducers near the midpoint of the wire span. These transducers detect deflection of the wires caused by an intruder cutting the wires, climbing on the wires to get over the fence, or separating the wires to climb through the fence. The wire is typically barbed wire, and the transducers are mechanical switches, strain gages, or piezoelectric elements. Taut wire sensor fences can either be mounted on an existing set of fence posts or installed on an independent row of posts.

Fiber-optic, mesh fences. Fiber optics can be woven into a mesh that can be installed on a fence to create a sensor fence. These mesh fences usually use some type of continuity detection to determine when an intruder has cut through the fence. The upper portion of the fence is usually configured mechanically in such a manner that the fiber is crimped when an intruder attempts to climb over the fence. The crimp of the fiber reduces the amount of light passed through the fiber causing an alarm.

Electric field or capacitance

Description. Electric field or capacitance sensors are active, visible, terrain-following sensors that are designed to detect a change in capacitive coupling among a set of wires attached to, but electrically isolated from, a fence.

Sensitivity and nuisance alarms. The sensitivity of some electric field sensors can be adjusted to extend up to 1 m beyond the wire or plane of wires. A high sensitivity typically has a trade-off of more nuisance alarms. Electric field and capacitance sensors may be susceptible to lightning, rain, fence motion, and small animals. Ice storms may cause substantial breakage and damage to the wires and the standoff insulators. Good electrical grounding of electric field sensors is important to reduce nuisance alarms. Other metal objects (such as the chain-link fence) in the sensor field must also be well grounded; poor or intermittent grounds will cause nuisance alarms.

Defeat methods. Because the detection volume extends beyond the fence plane, electric field

sensors are more difficult than other fence-associated sensors to defeat by digging under or bridging over the fence.

Performance. Electric field or capacitance sensors can be mounted on their own set of posts. This results in two areas of improved performance: a wider detection volume for the sensitive electric field sensor, and a lower NAR by eliminating extraneous motion from the chain-link fence. For the freestanding version of electric field sensors, some electronic signal processing techniques employ additional wires in the horizontal plane to reduce the effects of distant lightning and alarms due to small animals.

Freestanding sensors

General types

The types of freestanding sensors currently used for exterior intrusion detection are:

- Active infrared (IR).
- Passive infrared (PIR).
- Bistatic microwave.
- Video motion detection sensors.

Active infrared (IR)

Characteristics of exterior IR sensors. The IR sensors used for exterior intrusion detection are active, visible, line of sight, and freestanding sensors.

How IR sensors work. An IR beam is transmitted from an IR light-emitting diode through a collimating lens. This beam is received at the other end of the detection zone by a collecting lens that focuses the energy onto a photodiode. The IR sensor detects the loss of the received IR energy when an opaque object blocks the beam. These sensors operate at a wavelength of about 0.9 microns, which is not visible to the human eye.

Although single-beam IR sensors are available, multiple-beam sensors are normally used for high-level security applications because a single IR beam is too easy to defeat or bypass. A multiple-beam IR sensor system typically consists of two vertical arrays of IR transmitter and receiver modules. The specific number and configuration of modules depends on the manufacturer. Thus the IR sensor creates an IR fence of multiple beams but detects a single beam break. Multiple beam sensors usually incorporate some type of logic that will detect if an intruder attempts to capture a receiver with an IR source.

Nuisance alarms. Conditions that reduce atmospheric visibility have the potential to block the IR beams and cause nuisance alarms. If the visibility between the two arrays is less than the distance between the two arrays, the system will probably produce a nuisance alarm. These conditions sometimes exist in fog, snow, and dust storms.

Defeat methods. The detection volume cross section of a multiple-beam IR sensor is typically 5 cm wide and 2 m high; thus IR sensors have a narrow plane of detection similar in dimensions to fence sensors. IR sensors are considered line of sight sensors and require a flat ground surface, because the IR beam travels in a straight line. A convex ground surface will block the beam, and a concave surface will permit passing under the beam without detection. Digging under the bottom beam is possible unless a concrete sill or paved surface has been installed.

Passive infrared (PIR)

How PIR sensors work. Humans emit energy because of the warmth of their body. On the average, each active human emits the equivalent energy of a 50-watt lightbulb, and PIR detectors sense the presence of this energy and cause an alarm to be generated. For years, this technology was only usable in an interior application because the changes in heat emitted by the ground as clouds passed overhead caused too many false alarms. Current models, however, as shown in Figure 7, compare the received thermal energy from two curtain-shaped sensing patterns. A human moving into one area and then the other would cause an imbalance. Weather changes should affect both areas equally and would not cause an alarm.

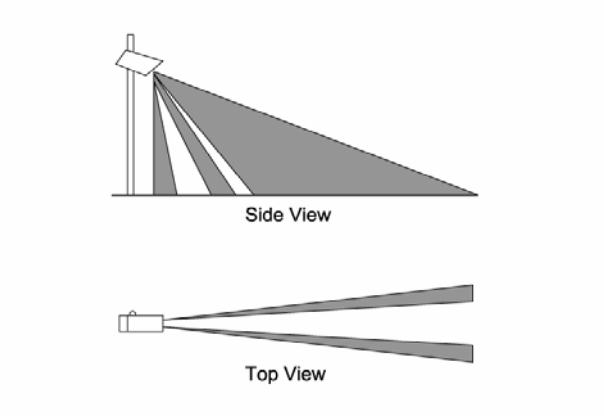


FIGURE 7. PIR sensor.

Nuisance alarms and detection ranges. The PIR sensors should be mounted such that the motion of the intruder will most likely be across the line of sight, because that is the most sensitive direction. Blowing debris, animals, and birds could cause nuisance alarms. The PIR detector is most sensitive when the background is at a much different temperature than an intruder. Detection ranges can exceed 100 m. Because these are optical devices, the only way to limit the maximum range is to aim the detector at a solid object, such as the ground, at the end of the desired detection zone.

Bistatic microwave

Description. Bistatic microwave sensors are active, visible, line of sight, freestanding sensors. Typically, two identical microwave antennas are installed at opposite ends of the detection zone. One is connected to a microwave transmitter that operates near 10 GHz or 24 GHz. The other is connected to a microwave receiver that detects the received microwave energy. This energy is the vector sum of the direct beam between the antennas and the microwave signals reflected from the ground surface and other objects in the transmitted beam.

Microwave sensors respond to changes in the vector sum caused by objects moving in that portion of the transmitted beam that is within the viewing field of the receiver. This vector sum may actually increase or decrease, as the reflected signal may add in phase or out of phase.

How microwave sensors work. Bistatic microwave sensors are often installed to detect a human crawling or rolling on the ground across the microwave beam, keeping the body parallel to the beam. From this aspect the human body presents the smallest effective object to the bistatic microwave sensor. This has the following important consequences for the installation of microwave sensors:

- *The ground surface must be flat* so that the object is not shadowed from the microwave beam, precluding detection. The surface flatness specification for this case is +0, –15 cm. Even with this flatness, crawlers may not be detected if the distance between antennas is much greater than 120 m.
- *A zone of no detection exists* in the first few meters in front of the antennas. This distance from the antennae to the point of first crawler detection is called the "offset distance." Because of this offset distance, long perimeters where microwave sensors are configured to achieve a continuous line of detection require that the antennas overlap one another, rather than being adjacent to each other. An offset of 10 m is typically assumed for design purposes, thus adjacent sectors must overlap twice the offset distance of 20 m.

Detection volume. The detection volume for bistatic microwave sensors varies with the manufacturer's antenna design but is large compared to most other intrusion sensors. The largest detection cross section is at midrange between the two antennas and is approximately 4 m wide and 3 m high.

Nuisance alarms. Microwave sensors tolerate a wide range of environmental conditions without producing nuisance alarms. However, nuisance alarms can be produced by the following conditions:

- A nearby parallel *chain-link fence with loose mesh that flexes in the wind* will appear to the sensor as a large moving target.
- *Surface water from rain or melting snow* appears to the microwave sensor as a moving reflector; therefore, the flat plane required for crawler detection should have a cross slope for water drainage.

- *Heavy blowing snow* may produce nuisance alarms. Snow accumulation will reduce the P_D, especially for the crawler, and complete burial of the antenna in snow will produce a constant alarm. The water content of the snow increases. Snow effects: dry light snow has less effect than heavy wet snow.

Defeat methods. Defeats by bridging or digging under are not simple due to the extent of the detection volume. More sophisticated defeat methods involve the use of secondary transmitters.

Monostatic microwave detectors. Monostatic microwave detectors are also available. In this configuration, the transmitter and receiver are in the same unit. Radio frequency energy is pulsed from the transmitter and the receiver looks for a change in the reflected energy. Motion by an intruder causes the reflected energy to change, causing an alarm. These sensors are "range-gated" meaning that the site can set the range beyond which motion can occur without an alarm. Monostatic microwave sensors have similar characteristics to bistatic sensors, although they are more affected by cross fences than parallel fences, and they are susceptible to re-aiming.

Dual technology sensors

Combine sensors to reduce nuisance alarms. In an effort to reduce nuisance alarms, dual technology sensors are becoming more popular for security use. An example of dual technology would be to place both a PIR and a monostatic microwave in the same housing. The device would not give an alarm until both sensors alarmed, thus avoiding common nuisance alarms from each of the technologies and only alarming on an actual intruder. In this mode, the sensitivity of each sensor could be set very high without the associated nuisance alarms.

The P_D of these dual-technology sensors is lower than some of the other sensors since an intruder must only defeat one of the two sensors to bypass the detector.

Video motion detection

Description. Video motion detectors (VMDs) are passive, covert, line of sight sensors that process the video signal from closed-circuit television (CCTV) cameras. These cameras are generally installed on towers to view the scene of interest and may be jointly used for detection, surveillance, and alarm assessment. Lighting is required for continuous 24-hour operation.

How VMDs work. VMDs sense a change in the video signal level for some defined portion of the viewed scene. Depending on the application, this portion may be a large rectangle, a set of discrete points, or a rectangular grid. Detection of human body movement is reliable except during conditions of reduced visibility, such as fog, snow, and heavy rain.

Nuisance alarms. Potential sources of nuisance alarms for VMDs used outdoors include:

- Apparent scene motion due to unstable camera mounts.
- Changes in scene illumination caused by such things as cloud shadows, shiny reflectors, and vehicle headlights.
- Moving objects in the scene such as birds, animals, blowing debris, and precipitation on or near the camera.

Defeat tactics. Defeat tactics include taking advantage of poor visibility conditions and camouflaging the target into the background.

Perimeter sensor systems

Integrating sensors into a system

This section discusses the integration of individual sensors into a perimeter sensor system and considers the interaction of the perimeter system or subsystem with a balanced integrated physical protection system. Before the detailed design and implementation of a perimeter sensor system are considered, some basic design philosophy and concepts for perimeter sensor systems should be understood.

Design concepts and goals

Continuous line of detection

By definition, a perimeter is a closed line around some area that needs protection. A design goal is to

have uniform detection around the entire length of the perimeter. This requires that sensors form a continuous line of detection around the perimeter. In practice, this means configuring the sensor hardware, so that the detection zone from one perimeter sector overlaps with the detection zones for the two adjacent sectors. Also, in areas where the primary sensor cannot be deployed properly, such as a gate, an alternate sensor is used to cover that gap.

Protection-in-depth

As applied to perimeter sensor systems, the concept of protection-in-depth means the use of multiple lines of detection. A minimum of two continuous lines of detection is used in high security systems. Many perimeter sensor systems have been installed with three sensor lines, and a few have four. For example, a perimeter sensor system might include a buried-line sensor, a fence-associated sensor, and a freestanding sensor. Multiple sensor lines provide duplicated detection, increased reliability and, in case of hardware failure, will provide fail-safe security. In this scheme, any single sensor can fail without jeopardizing the overall security of the facility being protected.

Complementary sensors

Significantly better performance by the perimeter sensor system can be achieved by selecting different and complementary types of sensors for the multiple lines of detection. Complementary sensors enhance the overall system performance, expressed in terms of the three fundamental sensor characteristics: P_D, nuisance alarm rate, and vulnerability to defeat.

This implies that no two sensor lines will use the same technology. This design philosophy results in detection of a wider spectrum of targets, allows operation of at least one sensor line during any conceivable environmental disturbance, and increases the difficulty of the task for the covert intruder attempting to defeat the system.

Priority schemes

Processing nuisance alarms. One disadvantage of multiple sensor lines is that more nuisance alarms will have to be processed. System effectiveness has not been increased if the system operator is overwhelmed with nuisance alarms because the P_D decreases as the time to assess alarms increases. The assessment subsystem should aid the operator in evaluating alarm information.

Using computer software to prioritize alarms. A recommended method for handling alarms requires the system operator to assess all alarms with the aid of a computer that establishes the time order of assessment for multiple simultaneous alarms. The computer sets a priority for each alarm based on the probability that an alarm event corresponds to a real intrusion. The alarms are displayed to the operator in order of decreasing priority; all alarms are eventually assessed. The alarm priority is established typically by taking into account the following:

- Number of sensors in alarm in a given sector.
- Time between alarms in the sector.
- Order in which the alarms occur in relation to the physical configuration of the sensors.
- Alarms in the two adjacent sectors.

Combination of sensors

Strive to improve detection and reduce nuisance alarms. It is desirable that a sensor or sensor system have a high P_D for all expected types of intrusion and a low NAR for all expected environmental conditions.

No single exterior sensor presently available meets both of these criteria. All are limited in their detection capabilities and all have high NARs under certain environmental conditions.

Basic techniques

The two basic techniques for combining sensors are:

- OR combinations.
- AND combinations.

OR combination. A system can consist of two or more sensors with their outputs combined by an OR gate so that an alarm would be generated when any sensor is activated. This combination is useful for sensors that make up for the deficiencies of each other, and each sensor is intended to detect particular types of intrusions. Thus sensors that detect aboveground, overhead, and tunneling

intrusions should be combined by an OR gate. The NAR of the OR combination (NAR (OR)) will be the sum of the NAR of each sensor.

AND combination. The NAR can be significantly reduced by combining sensors with an AND gate if the nuisance alarms of the sensors are not correlated. A seismic sensor and an electric field sensor do not give correlated alarms, for example, because they respond to different things. If both are activated at about the same time, it is probable that they have detected an intrusion.

Since a single intrusion attempt will not activate two or more sensors simultaneously, a system can be designed to generate an alarm if two or more sensors are all activated within a preselected time interval. A long time interval is desirable to assure detection of intruders moving slowly, but if the interval is too long, the NAR may not be reduced enough. By installing sensors so they cover the same general area, thereby providing redundant coverage, the time interval can be kept small.

AND combination and vulnerability to defeat. Detection probability of the AND combination (P_D(AND)) will be lower than the detection probability of each sensor. If an intruder can successfully defeat one sensor then the entire combination is defeated and will not alarm. To assure a reasonable detection probability for the system, the detection probability of the individual sensors must be high. AND combinations are seldom used in the exterior environment at high security facilities because of the vulnerability to defeat.

Clear zone

Definition and purpose. Two parallel fences extending the entire length of the perimeter usually define a clear zone. The fences are intended to keep people, animals, and vehicles out of the detection zone. The area between the fences is usually cleared of all aboveground structures, including overhead utility lines, and vegetation is also removed. After the zone between the fences is cleared, only the detection and assessment hardware and associated power and data lines are installed in the area.

The purpose of the clear zone is to improve performance of the perimeter sensor system by increasing detection probability, reducing nuisance alarms, and preventing defeat.

The clear zone also promotes good visual assessment of the causes of sensor alarms. A perimeter intrusion detection system performs better when it is located in an isolated clear zone.

Sensor configuration

Combine sensors to improve coverage. The configuration of the multiple sensors within the clear zone also affects the system performance. Overlapping the detection volumes of two different sensors within each sector enhances performance by creating a larger overall detection volume. As a result, defeat of the sensor pair is less probable because a larger volume must be bypassed or two different technologies must be defeated simultaneously. A third sensor can even further enhance performance, not by overlapping with the first two, but by forming a separate line of detection. Physically separate lines of detection can reveal information useful for determining alarm priority during multiple simultaneous alarms. In particular, the order of alarms in a sector (or adjacent sectors) may correspond to the logical sequence for an intrusion.

Site-specific system

Each site is unique. Each site requiring physical protection has a unique combination of configuration and physical environment. A physical protection system designed for one site cannot be transferred to another.

Factors that help determine which sensors will be appropriate. The following factors generally help determine the appropriate set of sensors:

- *The physical environment* will influence the selection of types of sensors for perimeter sensor systems.
- *The natural and industrial environments* provide the nuisance alarm sources for the specific site.
- *The topography of the perimeter* determines the shapes and sizes of the space available for detection, specifically the clear zone width and the existence of flat or irregular terrain.

Although the understanding of the interaction between intrusion sensors and the environment has increased significantly in recent years, it is still

advisable to set up a demonstration sector on site using the possible sensors before making a commitment to a complete system. This test sector located on site is intended to confirm sensor selection and to help refine the final system design.

Tamper indication

Features of tamper indication. The hardware and system design should incorporate features that detect or indicate tampering, as follows:

- Sensor electronics and junction box enclosures should have tamper switches that alarm if opened.
- Aboveground power and signal cables should be installed inside metal conduit.
- Alarm communication lines should use some type of line supervision that detects lines that have been cut, disconnected, short-circuited, or bypassed.
- To reduce vulnerability to defeat, place bistatic sensors so that an intruder must be in or pass through the detection volume to approach the receiver.

Self-test

Manual and remote testing capabilities. To verify normal operation of a perimeter sensor system, its ability to detect must be tested regularly. Although manual testing is recommended, manpower requirements are usually restrictive. A capability for remote testing of trigger signals can be provided and initiated by the alarm communication and control system. Typically this is just a switch closure or opening. In an automatic remote test procedure, the central computer control system generates at a random time a test trigger to a given sensor. The sensor must then respond with an alarm. The control system determines if an alarm occurred within a specified time and if it cleared within another specified time. Failure to pass the test indicates a hardware failure or tampering and produces an alarm message.

Pattern recognition

Computers can analyze pattern signals. Computers can receive signals from sensors and analyze the signal pattern, looking for patterns that are characteristic of an intruder. Using neural network or artificial intelligence software, the computers can learn the intruder signal patterns and then avoid nuisance alarms. Any sensor or combination of sensors that return a signal other than just "off" or "on" can have their signal analyzed by a computer and it can very reliably sense whether or not an intruder is present. One concern with these types of sensors is how the pattern recognition system is trained. It may be possible to over-train a system to reduce nuisance alarms at the expense of missing real intrusions. Another concern is that the intruder may be able to simulate a signal that the system rejects as a nuisance alarm in order to defeat the system.

Effects of physical and environmental conditions

The physical and environmental conditions that can affect exterior detection systems include:

- Topography.
- Vegetation.
- Wildlife.
- Background noise.
- Climate and weather.
- Soil and pavement.

These conditions are different at every site.

Topography. Topographic features such as gullies, slopes, lakes, rivers, and swamps must be considered when designing an exterior detection system. Grading may be required to reduce hills and slopes. Draining may also be required to reduce water flow through gullies and ditches to prevent seismic disturbances caused by running water. The perimeter system should avoid lakes, rivers, and swamps, since there are few commercial sensors suitable for use in water.

Vegetation. Sensor performance can be affected by vegetation in two ways: underground and aboveground. Motion of trees or plants caused by wind may be transmitted to their root systems and cause a seismic sensor to generate a nuisance alarm. Aboveground, an intruder can use large plants and trees as cover. If vegetation is a problem, mowing,

removal, soil sterilization, or surfacing should be used to control it.

Wildlife. In some locations, wildlife may cause problems. Large animals may damage equipment by collision and burrowing animals may eat through cable insulation material. Small animals, birds, and insects also cause nuisance alarms that may be difficult to assess. Dual chain-link fences and chemical controls may be used to control wildlife; however, local regulations should be observed with regard to poisons and repellents. Removing vegetation from fence lines has been found to discourage some smaller animals.

Background noise. A site survey along with information obtained from utility companies and plant-engineering organizations on site may reveal many sources of background noise. These sources may include wind, traffic, electromagnetic interference, and seismic sources:

1. *Wind.* These disturbances are caused by the transfer of energy to the ground by trees, power and light poles, fences, etc. High winds and windblown debris can also cause nuisance alarms from sensors mounted on fences by disturbing the fence.
2. *Traffic* from nearby roadways, railways, and airports creates nuisance alarms from seismic sensors. Roads should be kept smooth and the speed limit at a minimum to reduce the nuisance alarm rate. Seismic sensors are not practical near heavy air or railway traffic, because this type of traffic causes seismic disturbances even at long distances.
3. Examples of sources of *electromagnetic interference* include lightning, radio transmitters, welding, and electrical transients. Shielding of the sources or the sensors can reduce nuisance alarms.

Climate and weather. Specific data about the climate and the weather conditions should be obtained for the site. Information such as frequency, velocity, accumulation, and duration should be obtained about hail, electrical storms, rainfall, and wind. Mean minimum and maximum temperatures should also be noted as well as other weather and environmental conditions.

Because exterior sensors are installed outdoors, they are exposed to electrical storms at most sites. Lightning can easily disable, damage, or destroy the sensitive electronics used in sensor equipment. There are three primary precautions for reducing lightning damage. First, all signal cables should be shielded, either by the internal cable construction or by using metal conduit. Second, a good ground system is required. This means eliminating ground loops and using grounds at a single point. Third, passive transient suppression devices can be installed at the ends of the cables. Fiber-optic transmission cables are not affected by lightning and have thus become very popular for transmitting signals long distances outside a building.

Soil and pavement. Soil and pavement conditions can affect the operation of buried seismic sensors. The seismic conductivity of the medium is the determining factor. It should be high enough to make seismic sensors effective, but not so high that it causes nuisance alarms. Wet soil tends to have exceptionally good seismic conduction. However, wet soil tends to respond strongly to distant sources of seismic activity and thus cause excessive nuisance alarms. Buried systems of seismic magnetic sensors and seismic sensors may have to be embedded in or installed under areas paved with concrete or asphalt. The sensitivity of a sensor embedded in the pavement is increased if the sensor is adequately coupled to the medium. If the sensor is not adequately coupled to the medium, its sensitivity may be much lower than when it is installed in soil or buried under the pavement.

Integration with video assessment system

Compatibility

Many perimeter security systems use a CCTV system to perform alarm assessment. For both the sensor and video systems to perform well, care must be taken to ensure that the designs of the two systems or subsystems are compatible.

Clear zone

One consideration is the width of the clear zone. Sensor engineers desire a wide area for installing their sensors to reduce nuisance alarms. Video engineers desire a narrow area to assess so that they

can achieve better resolution from the cameras. A compromise clear zone width is in the range of 10 to 15 m.

Location of camera towers

Another trade-off is the location of the camera tower within the clear zone. The camera must be positioned to view the entire area being assessed. The sensors must be placed far enough away from the camera towers to prevent distortion of the detection volume and nuisance alarms. Frequently the camera towers are located 1 to 2 m inside the outer fence of the clear zone.

Integration with barrier delay system

Delay time allows video assessment

Balanced integrated physical protection systems usually incorporate some type of barrier or access denial systems to provide delay time for video assessment of the alarm source and for the response force to respond to an intrusion. In many cases, this includes some type of barrier installed at the perimeter; however, the barrier should not degrade the performance of the sensors.

Barrier placement

Perimeter barriers are usually installed on or near the inner clear zone fence so that an intruder cannot tamper with or defeat the barrier without first passing through the detection zone. This placement is important to ensure that the response action is initiated before the delay occurs. Barriers should not distort the sensors' detection volume, cause nuisance alarms, or obscure part of the cameras' view.

Summary

Exterior intrusion detection sensors have been discussed in terms of application, P_D, nuisance alarm rate, and vulnerability to defeat. The designer integrating individual sensors into a perimeter sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the perimeter system with a balanced and integrated physical protection system.

Section 8 – Recommendations

The following recommendations should be included in the design of a security system for a carcass disposal operation.

- **Plan ahead!** Before there is an incident, each level of jurisdiction should plan for the security system. Planning before an event will save costs during an event. Without advance planning the only immediate options are to fail to provide security (which may result in unacceptable health, financial, political, and other risks) or to incur very high labor costs. Advanced planning will help control the costs of security as well as provide a higher level of security.
- **Include local law enforcement in planning.** Local law enforcement should be included in the development of plans because they may be involved in implementation or other coordination with the carcass disposal operators.
- **Focus on low-cost, rapidly deployable technologies**.
- **Provide pre-event training.** All entities involved in security operations should train together. Training materials can be developed before an event so that they can be rapidly deployed to enforcement officials after an incident occurs.
- **Coordinate efforts.** Before an event, all relevant enforcement agencies should have plans for how to coordinate.
- **Understand the legal issues.** An understanding of the legal issues and the legal authorities of those involved in security should be in place prior to an event. There may be complex legal issues associated with seizing private property and implementing disposal operations on privately owned land.

- **Integrate security plans with biosecurity.** A well-designed and implemented security plan will help to assure the biosecurity of the site. An adequate security plan will help to ensure that biosecurity protocols are being followed and decontamination procedures are not bypassed.

Section 9 – Critical Research Needs

- Develop practical, prototypic security plans and then test them at actual large-scale feedlots (e.g., in southwest Kansas).
- Develop actual security plans for various jurisdiction levels. Before there is an incident, each level of jurisdiction should plan for the security system. Planning before an event will save costs during an event. Advanced planning will help control the costs of security as well as provide a higher level of security.
- Conduct activities that include local law enforcement in planning. Local law enforcement should be included in the development of plans because they may be involved in implementation or other coordination with the carcass disposal operators.
- Investigate and identify low-cost, rapidly deployable technologies.
- Develop pre-event training materials. All entities involved in security operations should train together. Training materials can be developed before an event so that they can be rapidly deployed to enforcement officials after an incident occurs.
- Summarize legal issues in carcass disposal site security. An understanding of the legal issues and the legal authorities of those involved in security should be in place prior to an event. There may be complex legal issues associated with seizing private property and implementing disposal operations on privately owned land.
- Integrate security plans with biosecurity. A well-designed and implemented security plan will help to assure the biosecurity of the site. An adequate security plan will help to ensure that biosecurity protocols are being followed and decontamination procedures are not bypassed.

References

Drayer, D.D., Sonnier, C.S., Mangan, D.L., & Walford, F.J. (1990). Redundant and Independent Containment and Surveillance Systems. http://infoserve.sandia.gov/sand_doc/1990/900806.pdf#xml=http://sasr089.sandia.gov/search97cg. Albuquerque, NM: Sandia National Laboratories.

Garcia, M.L. (2001). The Design and Evaluation of Physical Protection Systems. Albuquerque, NM: Sandia National Laboratories.

Sandia National Laboratories. (2003). Workshop Materials from the 2nd International Training Course on Physical Protection of Nuclear Facilities and Materials — all modules. Albuquerque, NM: Sandia National Laboratories.

Woodall, T.D. (2002). Security risk assessment overview: protecting our nation from evolving threats. http://infoserve.sandia.gov/sand_doc/2002/022204p.pdf#xml=http://sasr089.sandia.gov/search97cg. Albuquerque, NM: Sandia National Laboratories.