Security PACE Book 2 - Physical Security Concepts

Course Introduction

Physical Security Concepts

Physical Security Controls

Design Considerations for Physical Security

Barriers as a Means of Access Control

Preventing Interruption of Operations

Perception as Protection

Protection Scheme Guidelines

Lighting Application Issues

Physical Security Concepts is Book Two in this PACE series on Security Basics. It covers issues related to Physical Security as a key component of a comprehensive organizational approach to security.

Learning Objective

After completing this PACE Book, you should be able to:

- describe the goals of physical security controls
- describe and compare the definitions of physical deterrence
- explain the design features of countermeasures
- list the goals of a physical security plan
- identify the goal of in-depth protection
- list the three (3) levels of barrier protection
- describe the three (3) types of barriers
- discuss the features of a disaster recovery plan
- list the factors used in a perception plan
- list and discuss the three (3) elements used in protection lighting
- identify the protection objectives of illusory techniques
- describe the components of incident response
- explain the three (3) functional objectives of protective lighting
- discuss the strategies of object illumination design

Use the Menu at left to navigate through the course.

Physical Security Controls

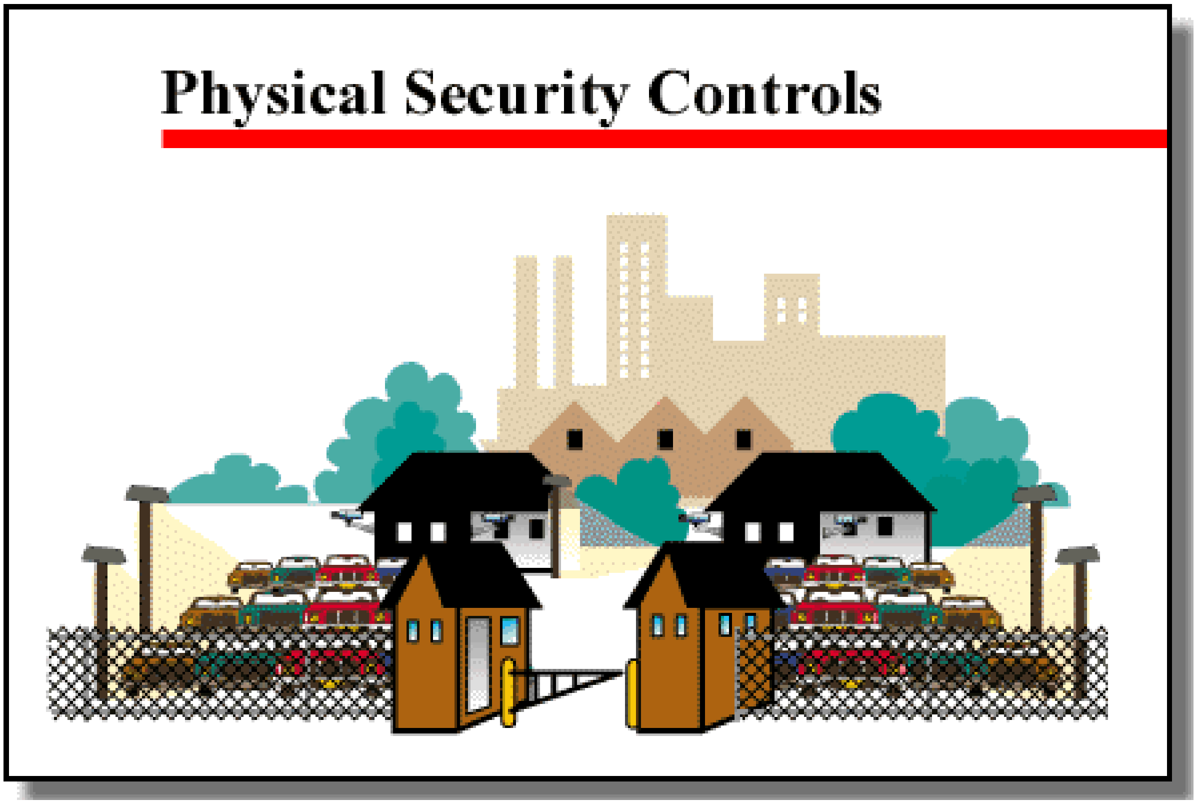
Physical Security Controls

Providing an organization or site with effective security involves several factors, some relatively obvious, others less so. The intent of Physical Security is to control access and prevent the interruption of operations. These goals are accomplished using tangible countermeasures ranging from fencing and lighting to electronic surveillance equipment and carefully defined policies and procedures.

Keep in mind that the actual Physical Security "controls" — the materials, equipment, and procedures used in securing a site — are only one element of an in-depth program of protection. Indeed, an effective component of many security systems is the perception of security both on the part of authorized personnel on site and potential intruders. Similarly, the use of barriers and lighting systems provide two important deterrents to potential intrusion:

- physical deterrence
- psychological deterrence, as a consequence of perceived impediments to successful intrusion

While an essential component of a comprehensive approach to security, Physical Security programs are only one aspect. To maximize effectiveness, security designers must include communications, access control, surveillance, and event reporting systems.



Physical Security Controls

Design Considerations for Physical Security

Design Considerations

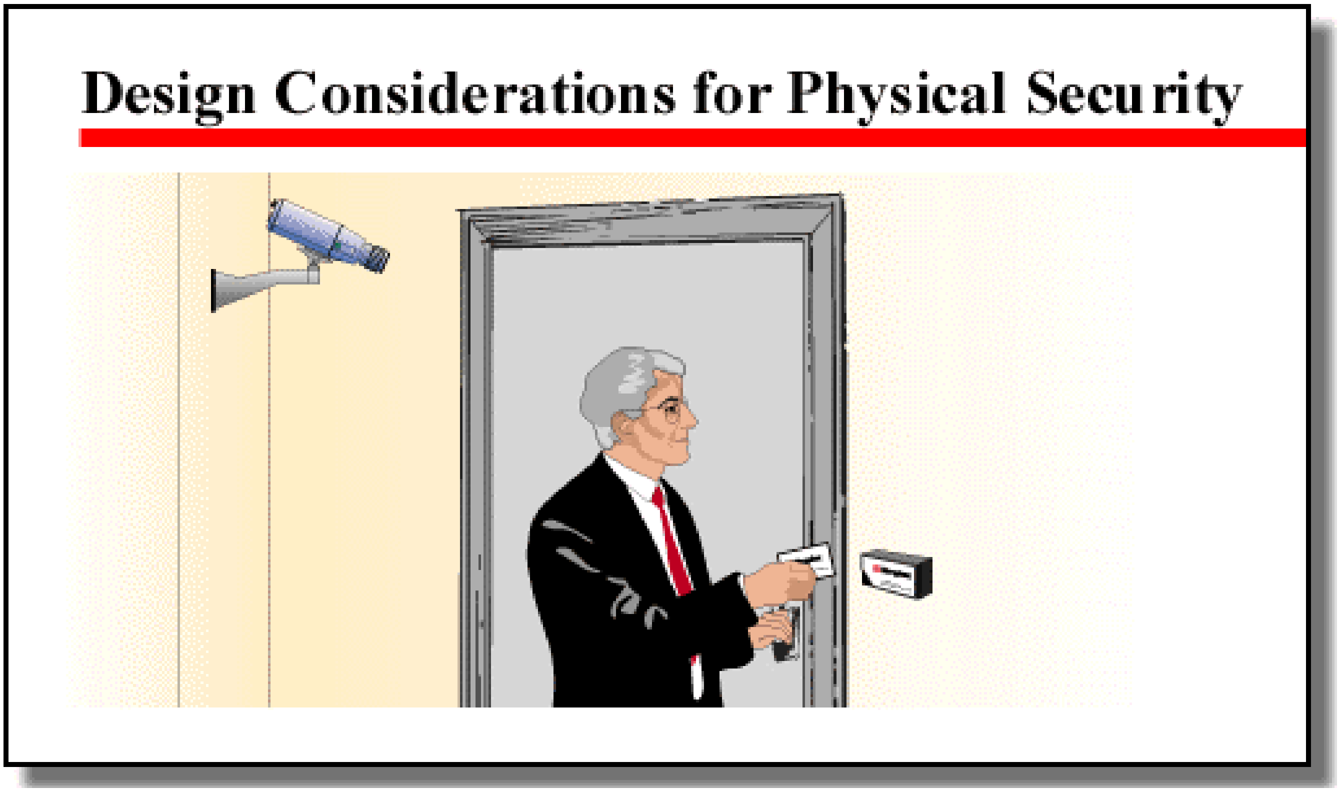
As mentioned above, Physical Security provides a "suite" of countermeasures designed to:

- ensure effective access control
- minimize the possibility of interruption of operations

In order to accomplish these goals, every Physical Security plan includes the following countermeasures:

- policies and procedures - comprehensive security goals and plans and how they will be implemented
- personnel - System administrators, operators, guards, etc.
- barriers which are access control systems or structures
- equipment including hardware and software, such as detection devices, alarm devices, communication systems
- records of historical and incident reports, access records and other logs

In the following two sections, we will pay particular attention to barriers as a means of providing effective access control, and methods for preventing operational interruptions. (Note: Book Five: Intrusion Detection Systems and Concepts and Book Six: Access Control Concepts discuss methodologies for protection of secured areas in more detail.)



Design Considerations for Physical Security

Barriers as a Means of Access Control

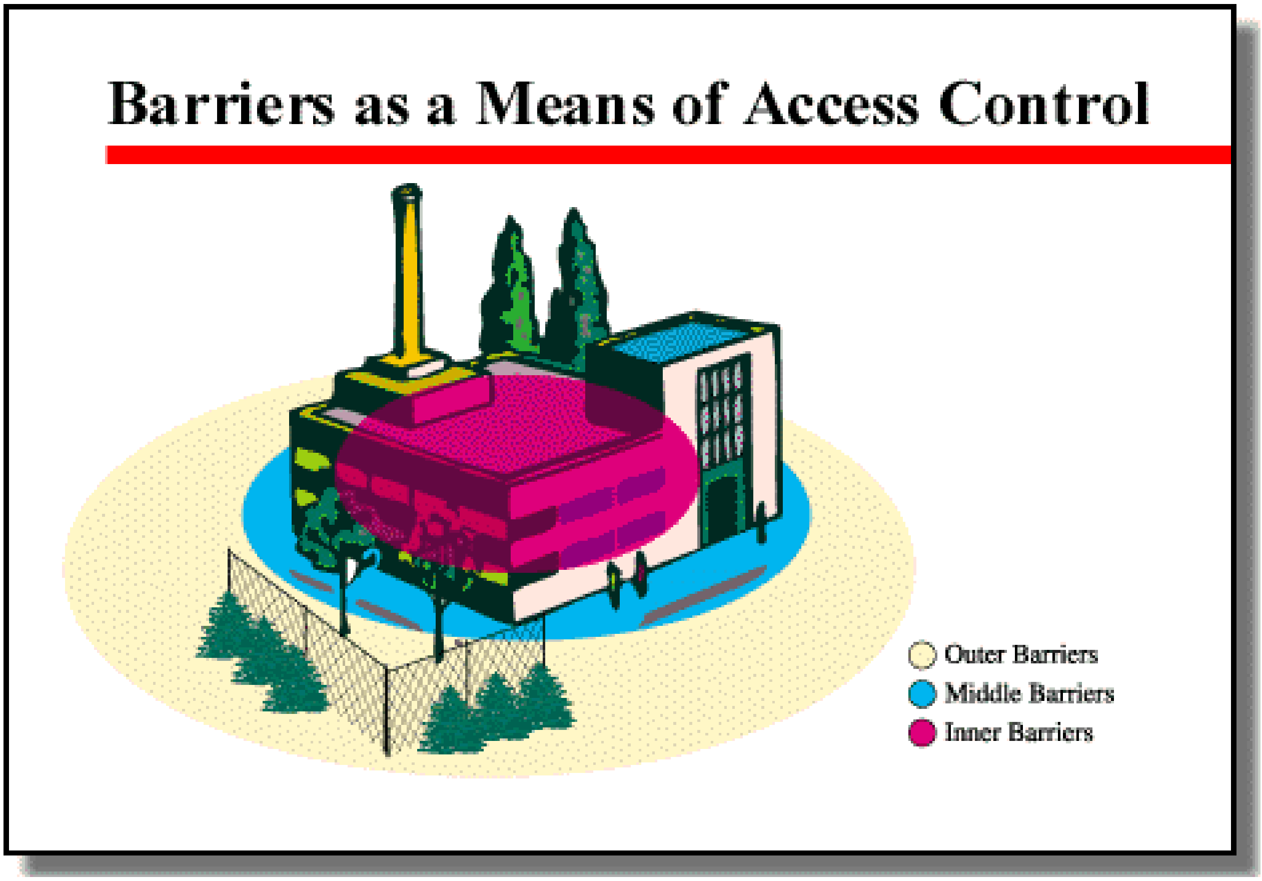
Barriers as a Means of Access Control

The goal of in-depth protection is achieved by controlling access through the use of barriers. Barriers are any means used to control the flow of access to an area. Barriers are typically arranged in concentric layers. The region which is the object of the protection is at the center, with the lowest level of security obviously residing at the outermost layer. Each layer closer to the center has a progressively higher level of security. The objective is to deter or delay an intruder as much as possible. In most security plans, three layers of barrier protection can be identified: outer, middle and inner.

Barriers define the physical limits of an area and prevent the penetration of that area by an intruder (either human or animal). Barriers are used to discourage penetration by accident, by force or by surreptitious means. Barriers should be designed to prevent an accidental penetration, constructed to defeat the expected force used in a penetration or to detect a penetration by stealth. Barrier should always be constructed with the understanding that additional countermeasures may be needed to improve the barrier's capability.

Barriers physically or psychologically deter or discourage the undetermined intruder, delays the determined intruder, and channel the flow of traffic through entrances. Barriers may be either natural or artificial (or structural). Natural barriers include bodies of water, mountains, marshes, deserts or other terrain difficult to traverse. Structural barriers are man-made entities such as fences or walls.

Every barrier can be compromised if enough time, money, personnel, planning, and imagination are used. To help counter such threats, multiple barriers are used in a physical security plan. A traditional security design known as "Security in depth," uses a series of barriers to prevent penetration.

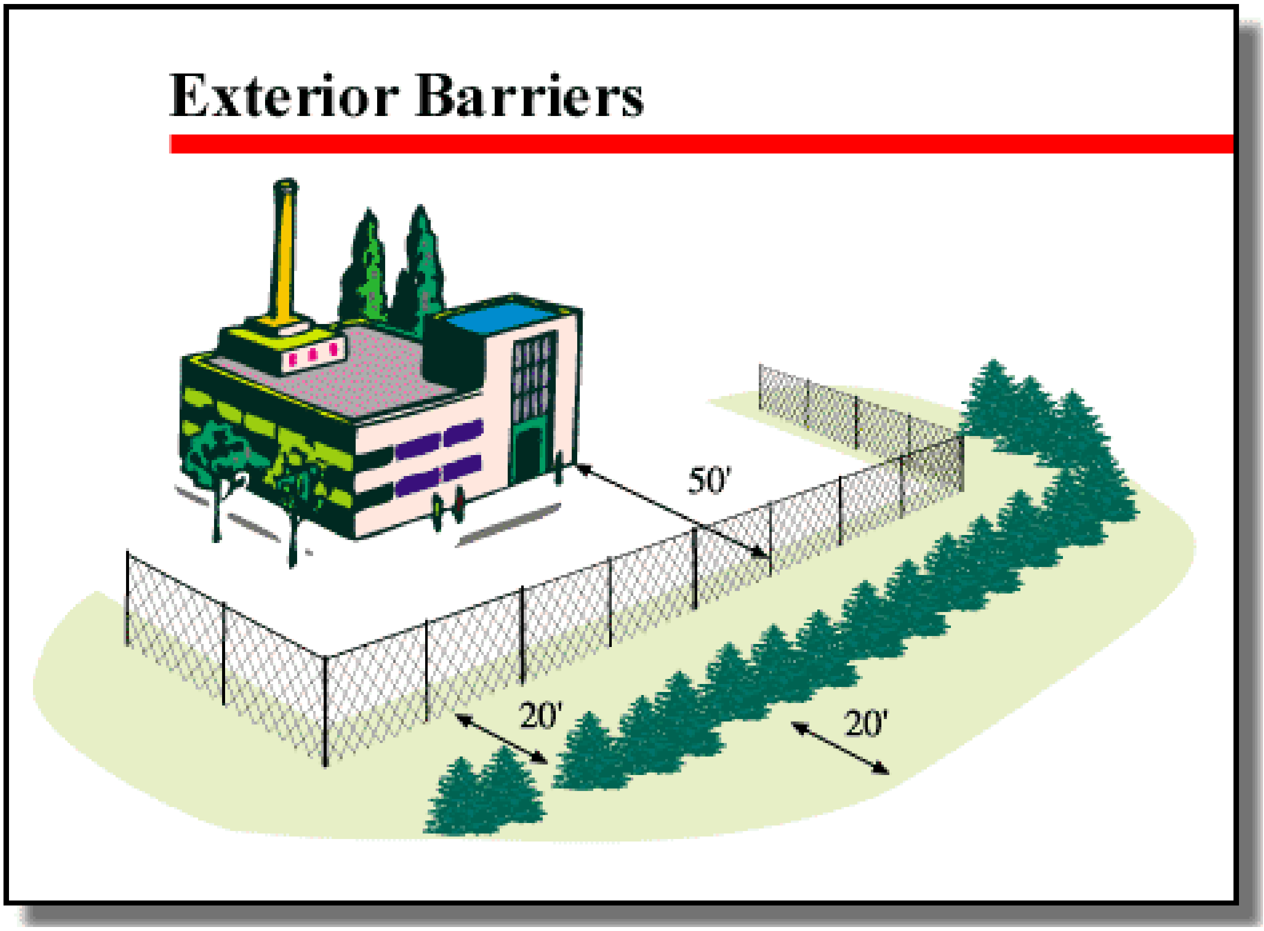


Barriers as a Means of Access Control

Exterior Barriers - Design Considerations

Exterior barriers (fences, walls, etc.) must include two "clear zones" - one on either side of the barrier. Each zone should be 20 feet or more of open space. The purpose of a clear zone is to provide an unobstructed view of the barrier and surrounding area. When a barriers surrounds a structure, a clear zone of at least 50 feet should be between the perimeter barrier and the structure. The exception to this rule is when a building wall forms part of the perimeter barrier.

Barriers are not only effective in preventing penetrations but they can also be used to control traffic (vehicles/pedestrians) flowing into or out of a facility. In addition to preventing intrusion, barriers should be designed to present evidence that a penetration has occurred. The goal here is to neutralize the effects of an intrusion and to prevent further entries. Ideally, evidence gathered at the barrier will provide data to designers for improvements in barrier planning and implementation.



Exterior Barriers

Building Surfaces as Barriers

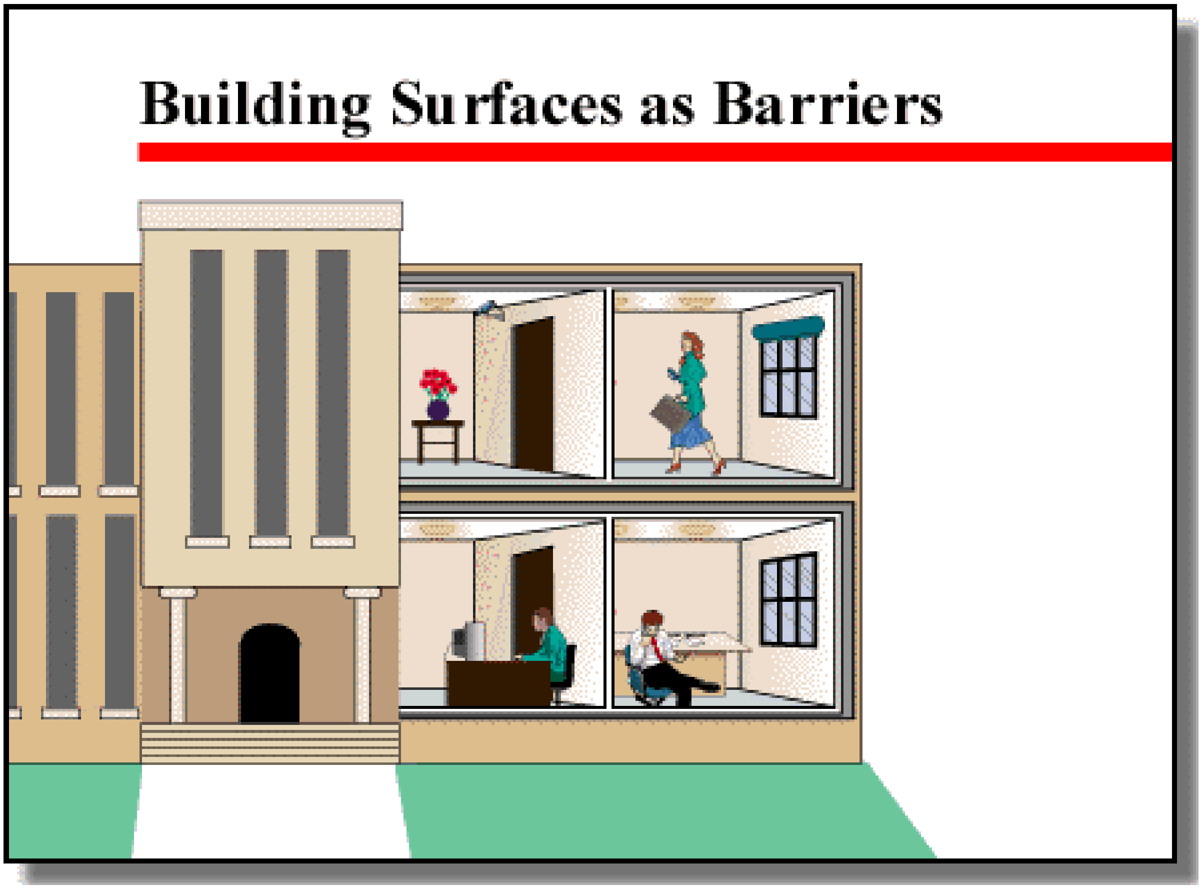
Building surfaces (walls, floors, ceilings, and roofs) are not typically designed to be barriers; however, such surfaces do deter penetration. For example, an exterior surface usually consists of at least two layers of material. While an exterior wall is primarily designed to address structural and environmental issues — building stability and comfort — such surfaces also serve to prevent intrusion.

Each building surface must be evaluated for its effectiveness as a structural barrier when used as part of the primary barrier. When evaluating building surfaces for security barriers, system designers must perform either a physical inspection of the surface or a review of the architectural and engineering drawings. It is recommended that both techniques be utilized whenever possible.

Perhaps the most significant weakness in building surfaces as security barriers are openings such as doors, windows, and overhead doors. Often their design pays only minimal attention to security issues. For example, typically, the frame or doorway serves only to hold a window or door in place. A frame or door jamb is not structural in that it is simply set into an opening in the building surface. As a result a doorway may be easily split and broken apart. In addition, the door itself it often weaker than the frame and may be easily compromised.

Another weak point may be the hinges. Inexpensive hinges or hinges installed without attention to security may be easily defeated, although when hinges are tampered with, evidence often remains.

Windows are usually designed to provide ventilation, natural illumination, visual access or a combination of the three. To harden windows when part of a barrier surface, glazing materials are used to strengthen the glass. Because glass has significant weaknesses, polycarbonate material or special plastic laminate between glass layers is used to reduce is susceptibility to penetration.



Building Surfaces as Barriers

The Three Layers of Barrier Protection

The outer protective layer may consist of fencing, natural barriers, lighting systems, signs, alarm systems. These controls generally accomplish two related functions:

- defining property lines
- channeling personnel and vehicles through designated access points.

The middle layer of barrier protection is usually considered to begin at the exteriors of any buildings on the site. Features may include:

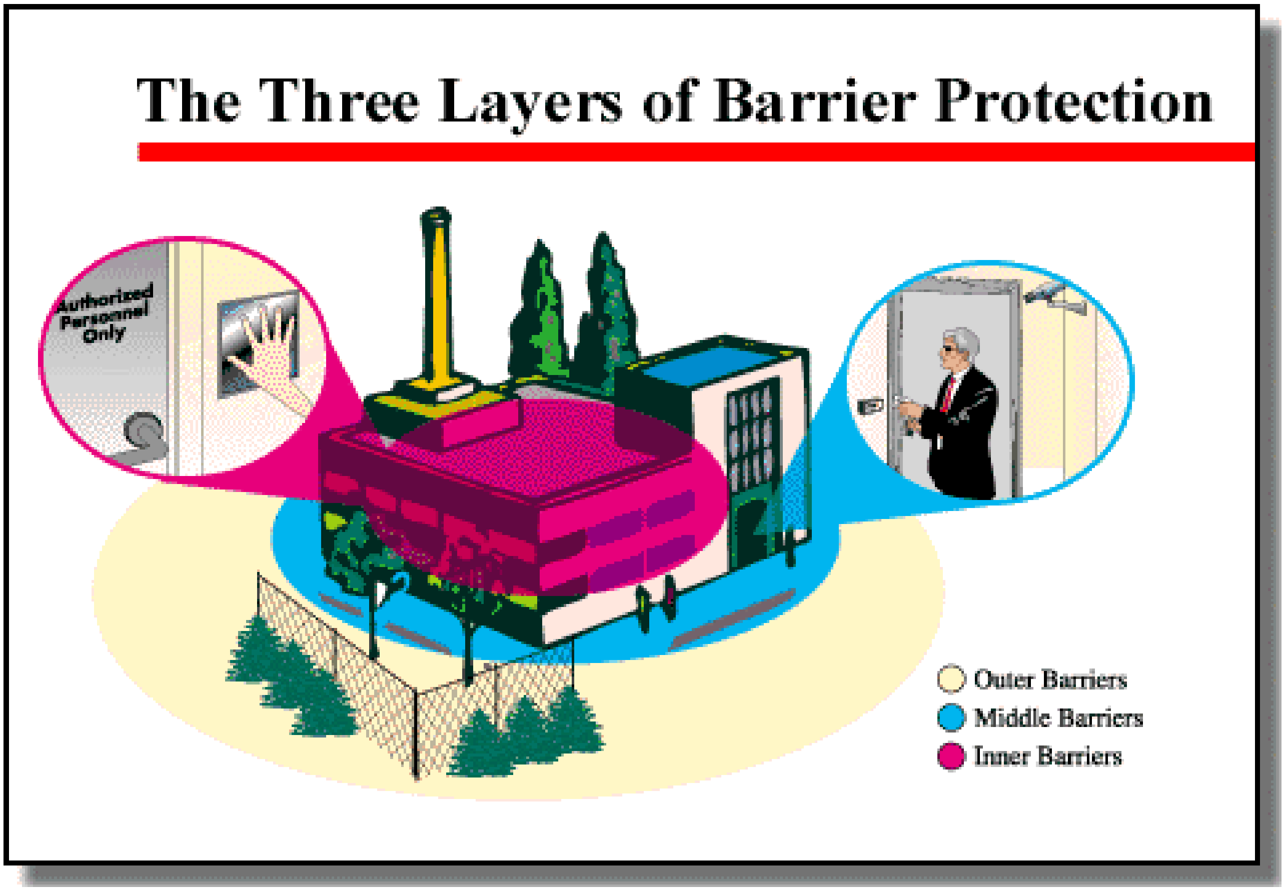
- lighting systems
- alarm systems
- locking devices
- bars or grillwork
- signs
- additional fencing.

More positive controls are used at this level than at the outer layer. Ideally, those planning security for a site must consider each building to be a six-sided box. Barrier design, therefore, should include provisions for protection from roof entry as well as intrusion from underground.

The inner lay may itself consist of several levels. This inner, and final barrier against intrusion will ensure that an intruder (any person attempting to enter a region who at any given moment may not be authorized to do so) will be detected even if the outer and middle layers of protection have failed to do so. Items or areas that could be protected are research/production data, equipment necessary to conduct operations, sensitive/competitive processes, negotiables, critical organizational records, computer rooms, etc.

The security design of the inner barrier layer also prevents the intruder from accessing anything deemed to have value. Features may include:

- window/door bars
- locking devices
- barriers, signs
- access/intrusion/alarm systems
- communication systems
- lighting systems
- safes and controlled areas



The Three Layers of Barrier Protection

Types of Barriers: Natural, Structural, Human

Effective barriers need not be necessarily man-made. (It is said a key factor in the low escape rate from Alcatraz Penitentiary in San Francisco Bay was the treacherous currents between the island and the mainland.) Barriers against intrusion may be naturally occurring, man-made, or human.

Natural barriers should be considered as part of a security plan. Natural barriers include:

- bodies of water, including rivers, creeks and lakes
- woods

- cliffs

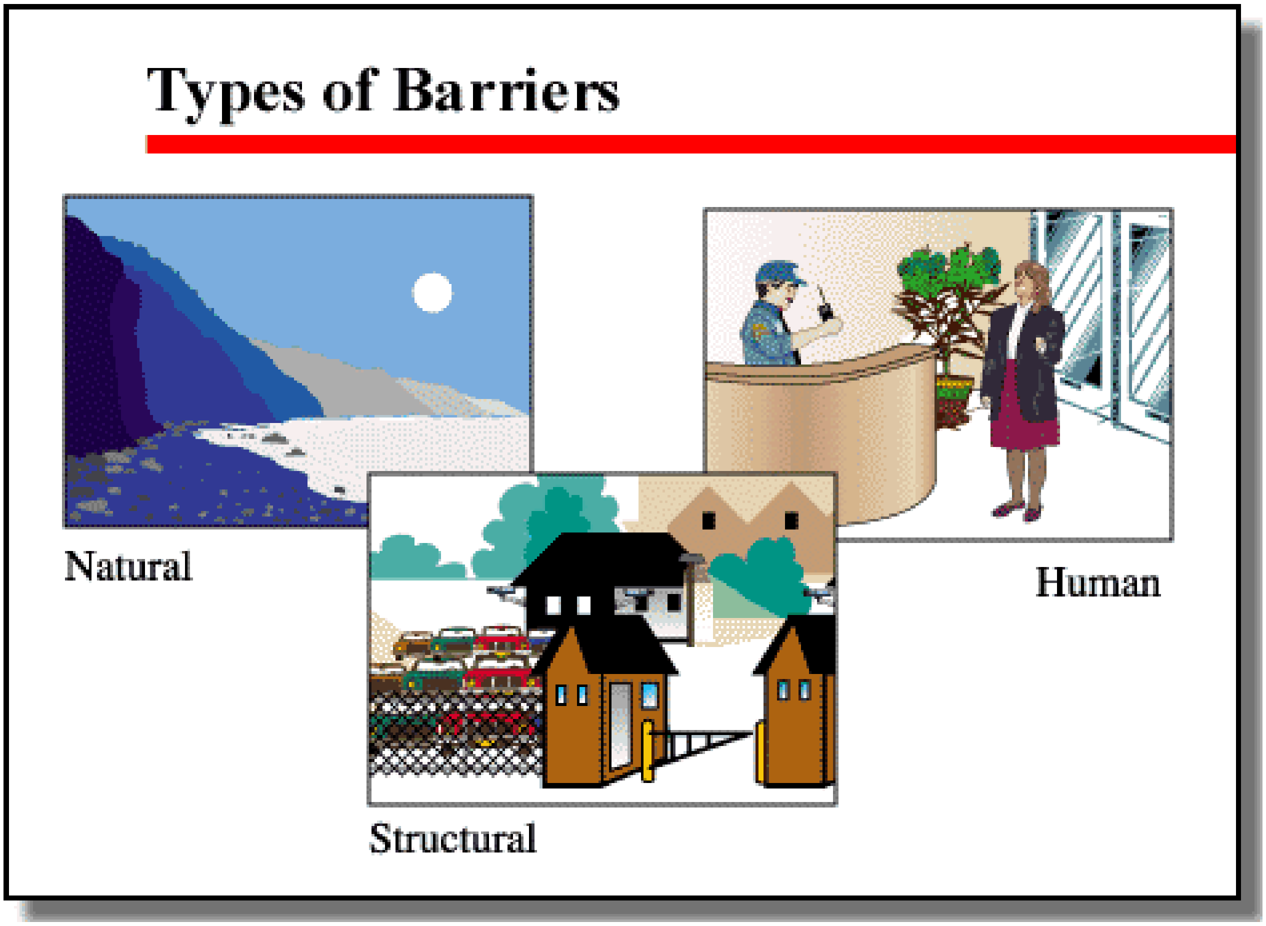
In addition to being effective outer layer barriers, natural barriers can be quite cost effective.

Structural barriers are man-made (or natural barriers manipulated by security designers). They are placed at strategic locations around a site to control access. Structural barriers include:

- Berms - manmade hillocks
- retention ponds
- planted tree lines to define boundaries
- walls
- fences
- doors, gates, and locking mechanisms
- ditches
- posts
- bollards - stanchions controlling traffic flow
- glazing materials.

The third type of barrier comes in the form of a human presence. Here the security design uses people to control access and limit movement areas. Human barriers may be in use in any of the three layers of barrier protection. Personnel used to provide human barriers include:

- public safety/police
- contract/proprietary security officers
- receptionists.



Types of Barriers

Natural

Human

Structural

Preventing Interruption of Operations

Preventing Interruption of Operations

For many organizations, it is not enough to keep unauthorized personnel out of secure areas. More is required. If operations are interrupted, the results can have a serious negative impact on the organization, its employees, the people it serves, and the community of which it is a part. Because of the importance of maintaining normal operations, minimizing the potential interruption of operations is the second major goal of an in-depth physical security plan. When thinking about interruptions to operations, sabotage and vandalism are certainly important security considerations; however, such interruptions can also be caused by natural disasters, environmental disasters, or industrial accidents.

A well-designed Physical Security plan must incorporate policies and procedures to ensure continued operations even should one of the above situations occur. A comprehensive approach to Physical Security must include disaster recovery plans. Such plans must include:

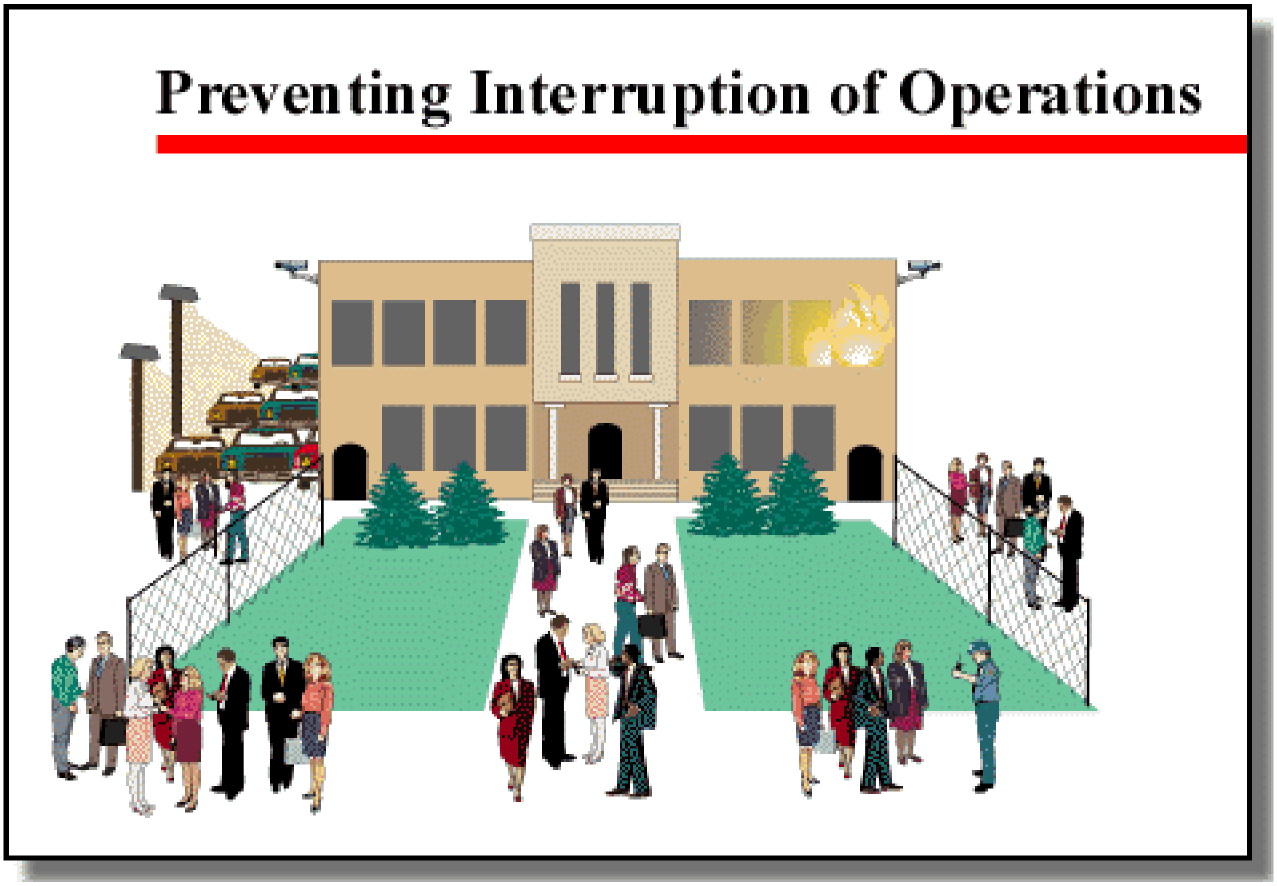
- evacuation procedures
- marshalling of resources to deal with the emergency event
- maintaining order on the site

- administering first aid and directing emergency services and operations
- the protection of assets (personnel and property).

The presence on-site of hazardous materials adds to the challenges and complexity of a disaster recovery plan. An event involving such materials may require a highly specialized response utilizing equipment and personnel far beyond the scope of non-Haz Mat events. Plans designed in response to potential hazardous material incidents must be developed with local and possibly even regional public safety assistance, being sure to meet local, state and federal environmental safety regulations. The plan must address issues such as:

- relocation of materials
- containing spills
- minimizing losses and contamination of personnel and property
- notification to proper authorities and employees
- securing affected areas to prevent unauthorized entry.

Preventing Interruption of Operations



Preventing Interruption of Operations

Perception as Protection

Perception as Protection

Clearly a major goal of any physical security plan is to ensure employees, customers, visitors and vendors are secure. In reality, accomplishing this goal requires security planners to look beyond the arrangement of barriers, the institution of access control, etc. Security personnel may know all prudent and expedient measures have been taken to ensure a high level of security. If, however, workers, customers, and others do not feel secure, then even the best efforts of the security department will have failed.

For a security plan to be truly effective, employees, customers, visitors and vendors must perceive they are secure; they must believe they are in a safe and secure environment. Consider the effect of a simple homeowner security device — a sign that read, "Beware of the Dog." You do not need to see the dog for it to have an effect. Designers of an effective security plan must recognize the key role "perception" plays in providing protection — and not just from the point of view of authorized personnel at a site, but from the viewpoint of potential intruders as well.

First, to incorporate elements in a security plan which will ensure a "perception of security," planners should begin by identifying factors and security issues that concern persons at work and visiting the site. What fears do these persons have and what are reasons for these fears?

Next, a physical security plan must involve all groups within an organization. From the start, security must be viewed by all as part of every employee's responsibility. All personnel must understand that they play an important role in the organization's security program.

Every element of the Physical Security Plan should be reviewed not only for its ability to reduce unauthorized entry and loss prevention but also its ability to create the perception of a safe and secure environment. To restate this, effective security protection consists not only of the actual measure taken, but also the perception of protection it presents. For example, U.S. Department of Defense studies have shown fencing topped with barbed wire can be breached by knowledgeable intruders in under ten seconds. For many people, however, this same fence may appear impossible or difficult to breach, and therefore will provide an initial deterrence.

In many organization, including retail store operations, security programs can be enhanced by the use of devices, such as signs and dummy CCTV cameras (e.g., the mirrored half-dome CCTV enclosure) to create or heighten the illusion of protection. An individual only has to see the dome — not any camera which may be inside it — to understand he or she may be under surveillance.

In summary, effective protection schemes must incorporate three approaches to security:

- visible with real protection
- not visible with real protection
- presenting the appearance of protection but in fact an illusion.

In the following sections we will provide more detail in designing such a protection plan.

Perception as Protection

WARNING
These premises protected by surveillance cameras. Shoplifting will be prosecuted.

Protection Scheme Guidelines

Select the first topic below to begin this lesson:

TOP

Protection Scheme Guidelines

Developing an effective Physical Security plan involves a series of logical steps. While the specific content developed during these steps varies from organization to organization, the basic steps remain the same. The first step is to perform a "Vulnerability Assessment." (This process was discussed in PACE Book One.) Based on this assessment, as developed for a particular organization, security planners can identify specific "protection objectives" for the organization. At this point, planners can determine what techniques and equipment will be required to accomplish the objectives. Included in this step is a determination of which objectives may be supported with illusory techniques.

Protection Scheme Guidelines

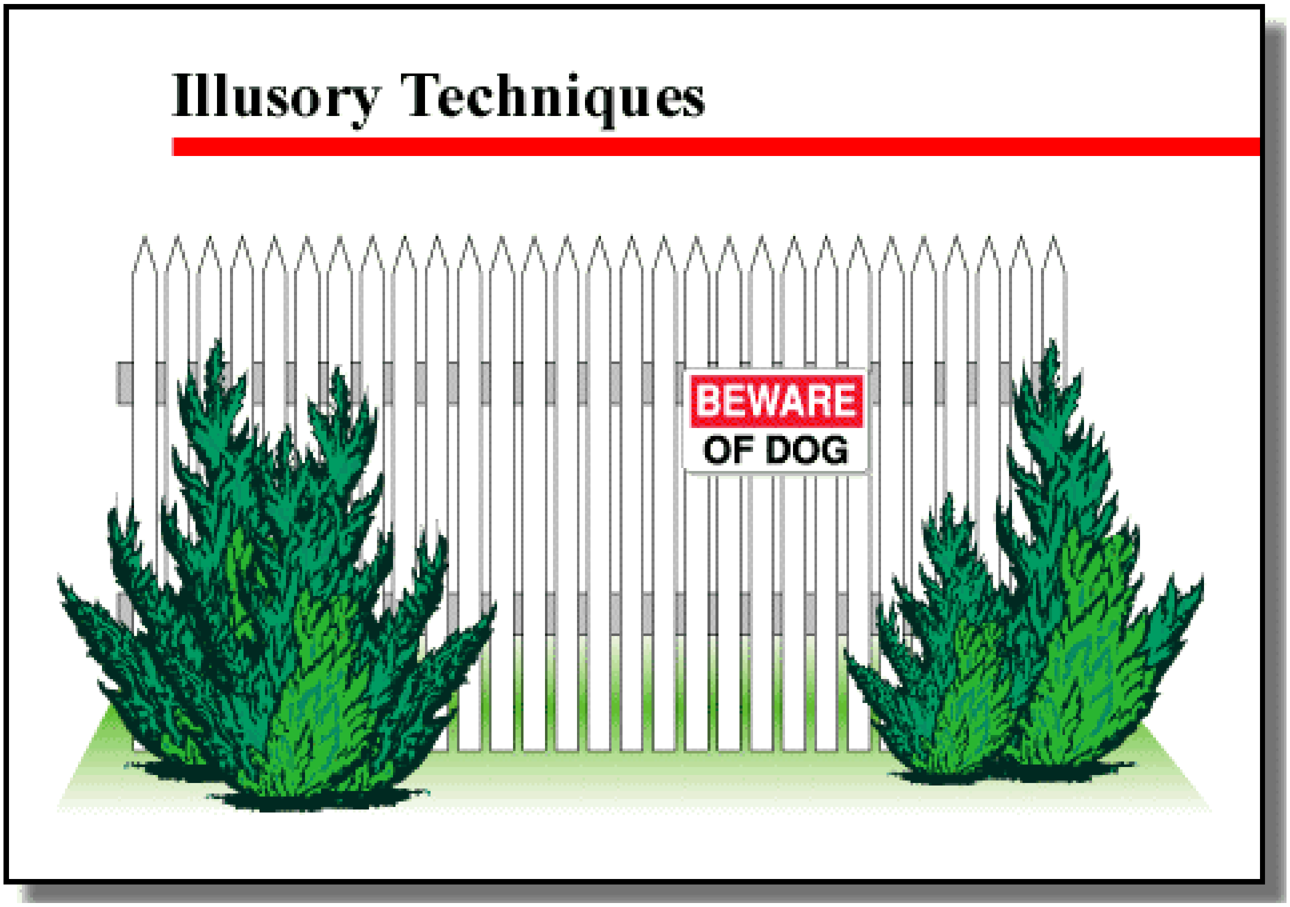
Guidelines for Illusory Techniques

Establishing the image of security requires an assessment of what types of illusions might be utilized and how they will relate to the tangible security assets of the program.

One word of caution, regarding illusory techniques: occasional failures of illusory techniques occur — as in shoplifting in a department store's ready-to-wear department. It may be that some loss is acceptable in such a store's security plan for that department. Now consider the same department store, but this time the jewelry department. Here any loss is deemed unacceptable. Armed with these two pieces of information, the security designers for the store can plan an appropriate security response to the potential threats. In the case of the ready-to-wear department, it may be that the use of simulated CCTV domes is appropriate. On the other hand, when it comes to the jewelry department, the same planners may call for a series of domes actually containing functioning CCTV surveillance cameras. At each location, appropriate signage warning of surveillance may further deter potential threats. Clearly in this setting, a variety of security options is appropriate. Therefore, real techniques (CCTV, alarm systems, and signage) in combination with illusory techniques (simulated CCTV domes) is deemed to provide effective levels of protection.

When these techniques are combined with procedures such as selected prosecution of violators (including publication of the court proceedings), the organization — in this case the store — can create a comprehensive and effective security plan.

A note of caution: once an illusory technique has been compromised, it has no further value and should be immediately discontinued. In order to prevent this from occurring, it is essential to keep the actual number of personnel who know the true aspects of the security plan to the absolute minimum.



Illusory Techniques

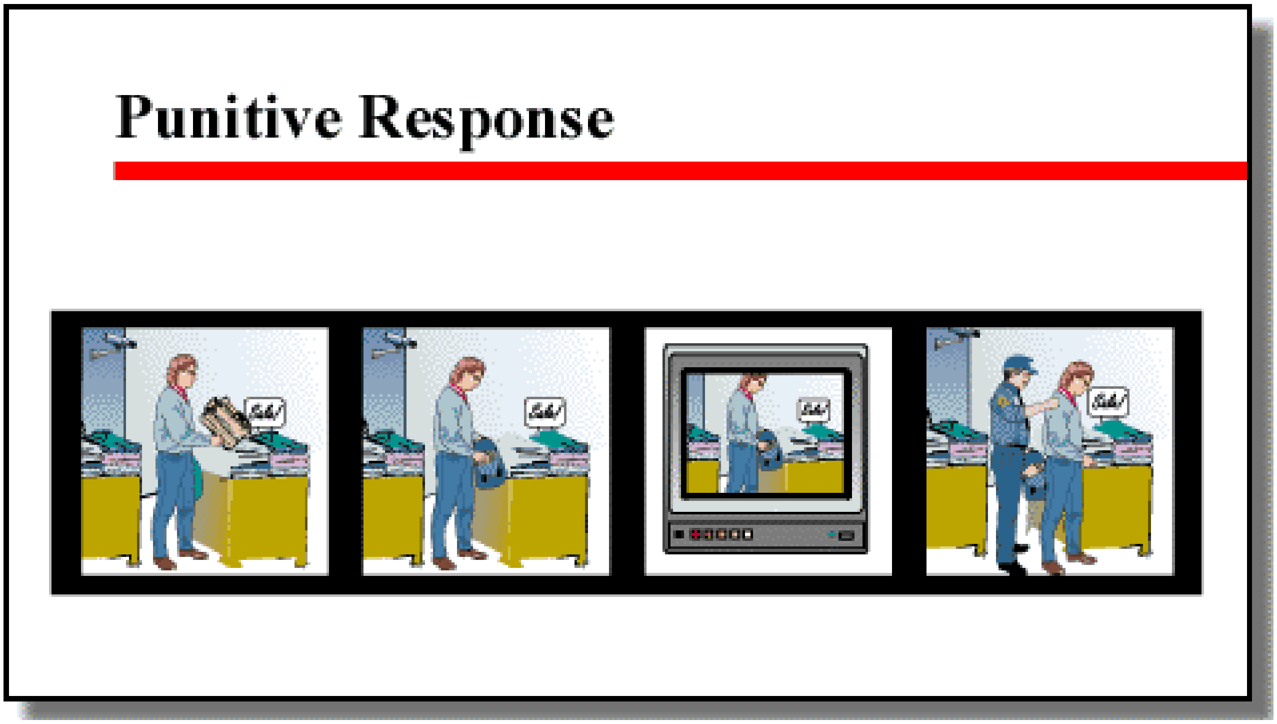
An Essential Ingredient: Incident Response

A key component to ensuring the on-going effectiveness of a security plan is the consistent and predictable response to any incidents that may occur. The security plan, therefore, should have clearly defined responses in place in the event of an incident. Such responses should be balanced in their effect. They must be designed to be both preventative (discouraging attempted threats) and punitive (punishing the current offender).

A preventative response is initiated before the unauthorized person reaches the protected objective. It is designed primarily to be a clear warning that additional response capabilities are in place. As such a preventative response is intended to discourage continued attempts and to turn away the intruder.

A punitive response is initiated once the penetration has occurred or is still in progress. Rather than turning away an intruder, the objective of punitive responses is the identification and apprehension of the perpetrator. An example of a punitive response is the capture of a robber resulting from a police response to a silent alarm from a bank.

Balanced response it the preferred methodology and involves both of the previous responses used singularly or in combination throughout the security plan.



Punitive Response

Cost Impact on Security Plans

A final consideration in a protection scheme is financial: available funds versus costs. Obviously sufficient funding must be available to provide adequate protection based upon the risk management profile. Funds must be sufficient to cover costs associated with personnel, training, equipment, and maintenance requirements. The cost of the system must be viewed in contrast to the potential cost of losses resulting from inadequate security measures. This kind of analysis can be an important aid as decisions are made regarding funding levels for an organization's security plan.

Cost Impact on Security Plans

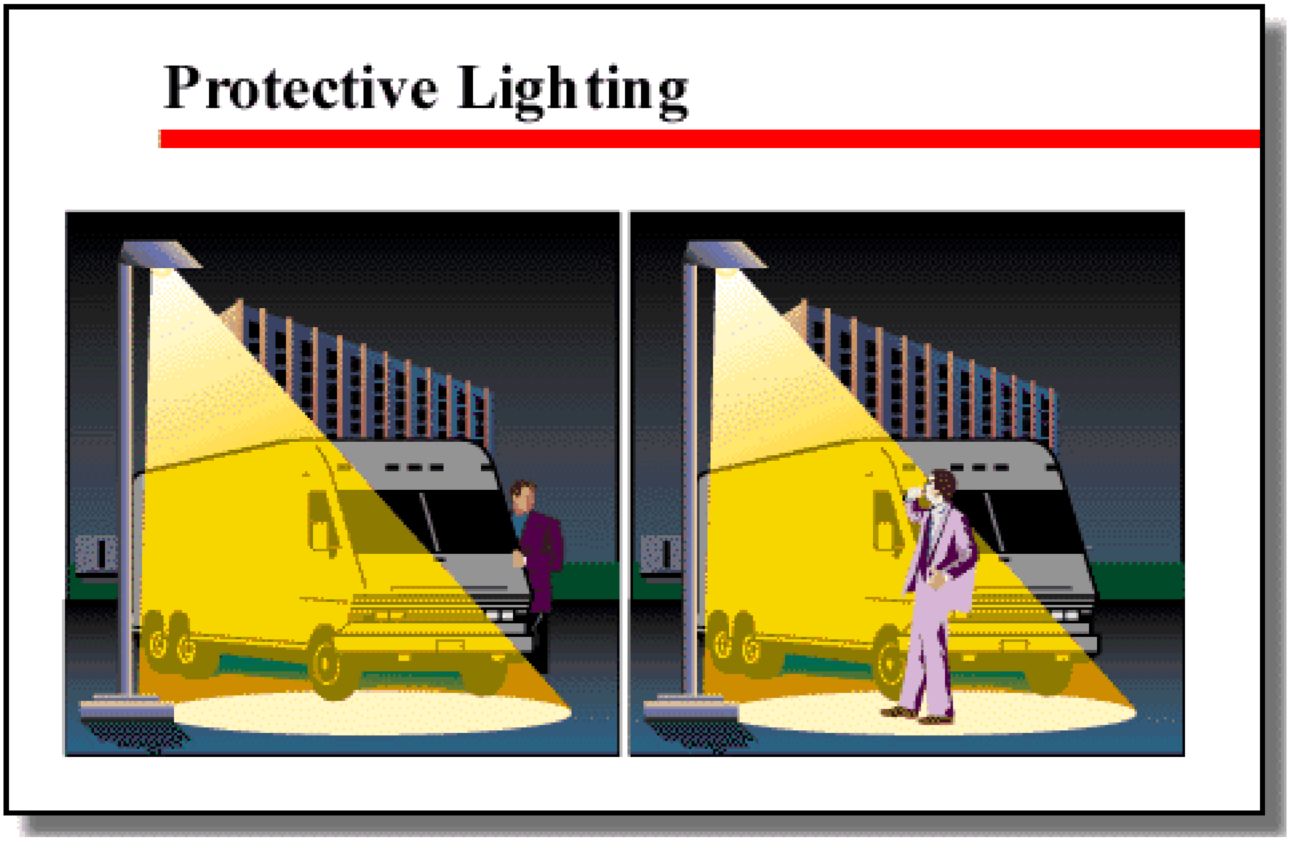
Guidelines for Protective Lighting

An important component of a comprehensive security plan is lighting. Security Protective Lighting has three functional objectives:

- to illuminate a person, object, place or condition of security to permit observation and identification

- to be a physical deterrent through the glare effect of direct light on the human eye

- to be a psychological deterrent creating in an intruder's mind the awareness that he or she will be discovered and observed during any unauthorized entry attempt.



Protective Lighting

Object/Area Illumination

The most obvious reason for protective lighting is to make certain any person, object, place or condition will be sufficiently illuminated to provide effective security in a given region. In order to assure sufficient illumination a number of conditions must be met. For example, lighting designers must consider natural properties of reflectance, light absorption capacity, mobility and an object's inherent sensitivity to light. All these factors affect an entity's visibility. Other factors to consider include:

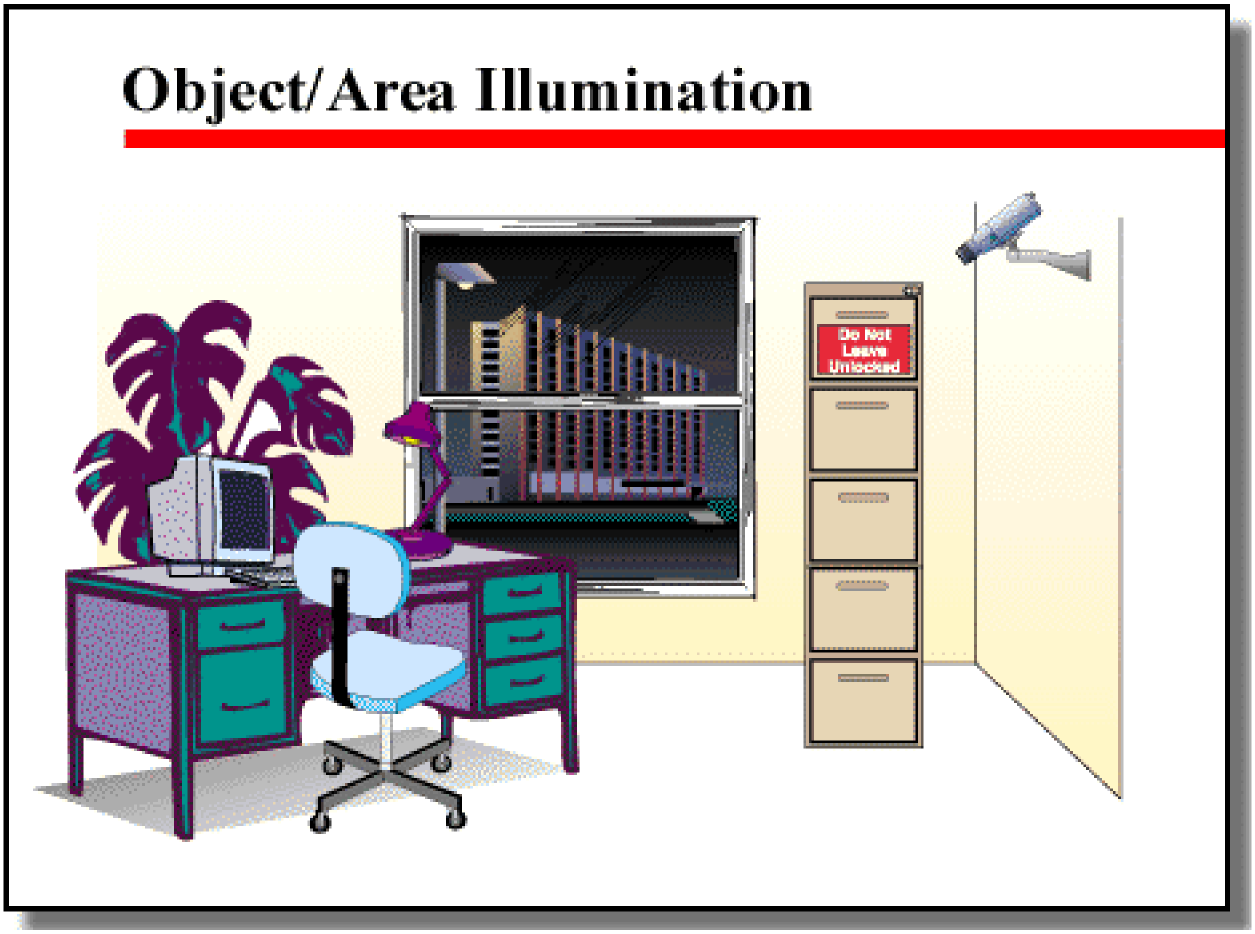
- the schedule of observation. Will the observation be constant or intermittent? If intermittent what will the frequency of observation be and will the observation be performed on a regular or random basis

- the means of observation. Will the observation be performed by a person or CCTV system? In either case, sufficient illumination must be available to accomplish the observation. For CCTV, the camera specifications will list required illumination.

- the area and quality of coverage. Is it necessary to observe all details in the area of coverage, or will only selected elements within the area be of interest? What level of detail is necessary? Is it necessary, for example, to observe changes in color? This clearly would affect decisions regarding the "quality" of the illumination, in this case color temperature, specifically.

- reliability of the illumination devices. If, for example, observation is to be constant, equipment mean time between failure rates as well as back-up power source must be considered. In addition, system designers must factor in restoration time of illuminating devices when a power failure occurs. Some lamps require several minutes of operation before they reach their specified levels of illumination output and quality.

When considering an illumination system for protection, the answers to these questions are essential in implementing a system which meets the organization's requirements.



Object/Area Illumination

Lighting as a Physical Deterrent

In addition to providing simple illumination in an area of coverage, protective lighting may be given a more "active" role in deterring intrusion. One factor in the effectiveness of lighting used in this manner is it's brightness and position in relation to the intruder. Earlier we referred to this as the "glare effect." Consider the disorienting effect (and therefore deterring effect) of suddenly filling an area with high levels of illumination triggered by an intrusion detection device. If this is a component of a lighting system design, note that such an effect may be enhanced by keeping an area in low light levels until an intruder is detected.

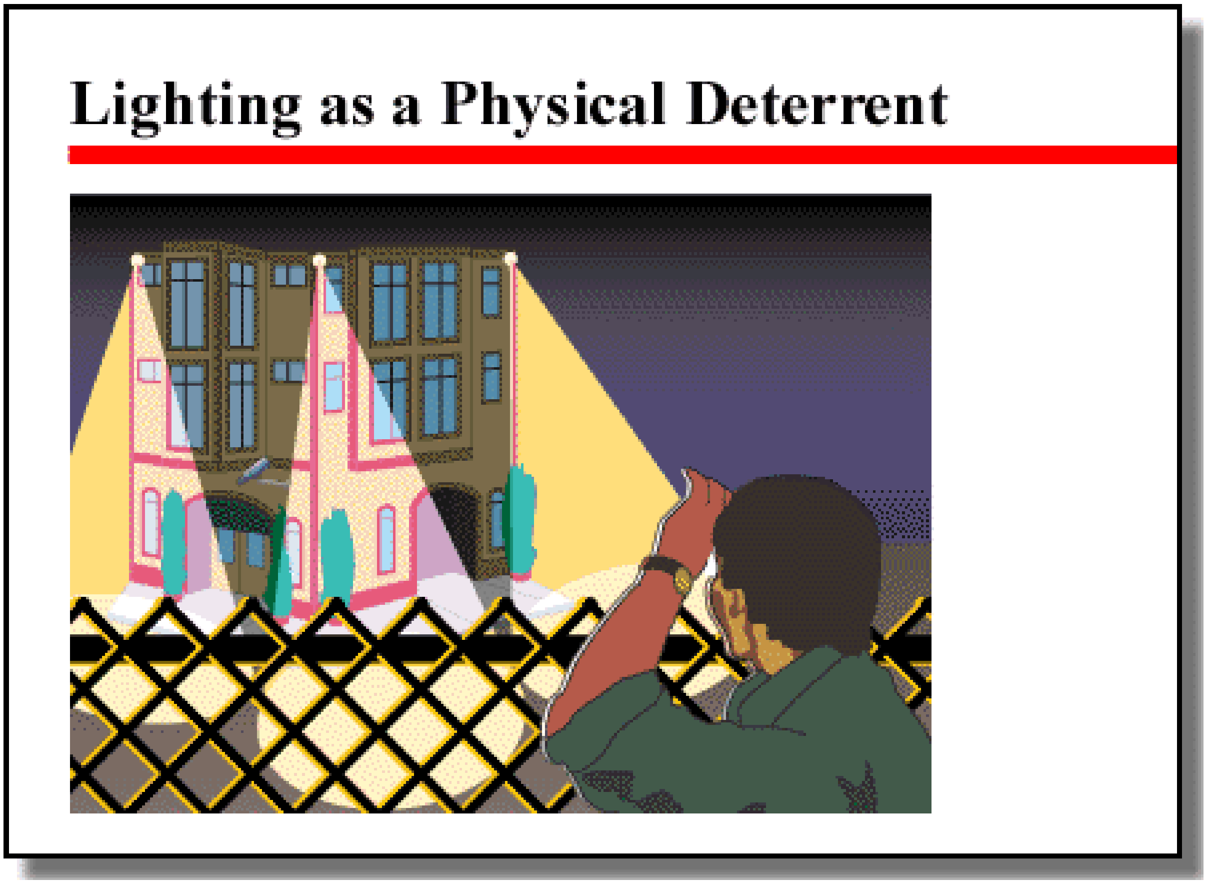
When protective lighting will be used as a physical deterrence, the following questions must be considered:

- Will the system be continuously deployed or event activated? It may be deemed useful to provide continuous illumination. (This may provide a psychological effect as well as actual.) On the other hand, depending on the area of coverage and design objectives, the lighting system may be event activated; that is, a specific event (detected intrusion, time period, etc.) may trigger the lighting system to be turned on.

- Will the system be target oriented or omni-directional? In some situation, it may be desirable to illuminate an entire area of coverage. In other settings and with different security requirements, target oriented illumination may be sufficient, providing, in effect, pools of light illuminating only specific objects or locations within the same area of interest.

- Will the protective lighting system be interface with CCTV or alarm systems?
  What failure rates of system components or simultaneous element failures are the most critical to overall system performance?

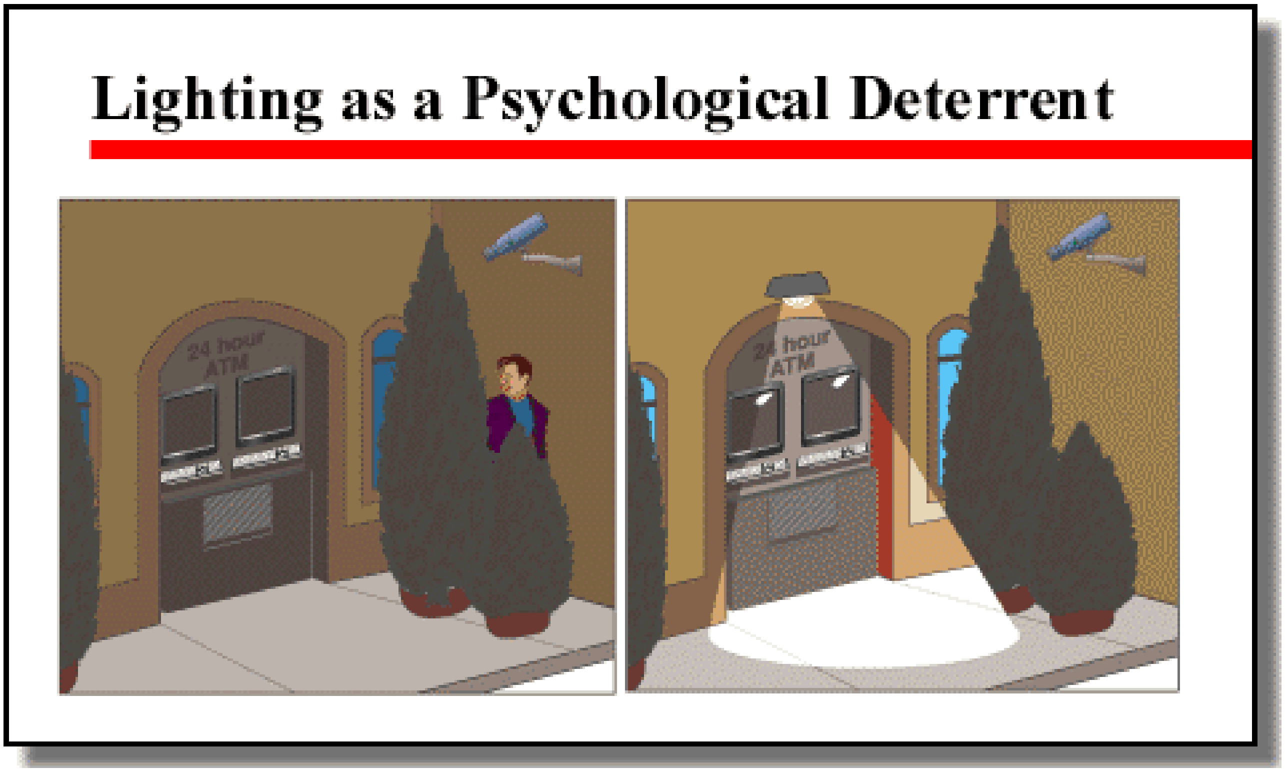
- Could the system be accidentally activated this causing an injury or damage? This is an issue that must receive special consideration it if is to be event activated.



Lighting as a Physical Deterrent

Lighting as a Psychological Deterrent

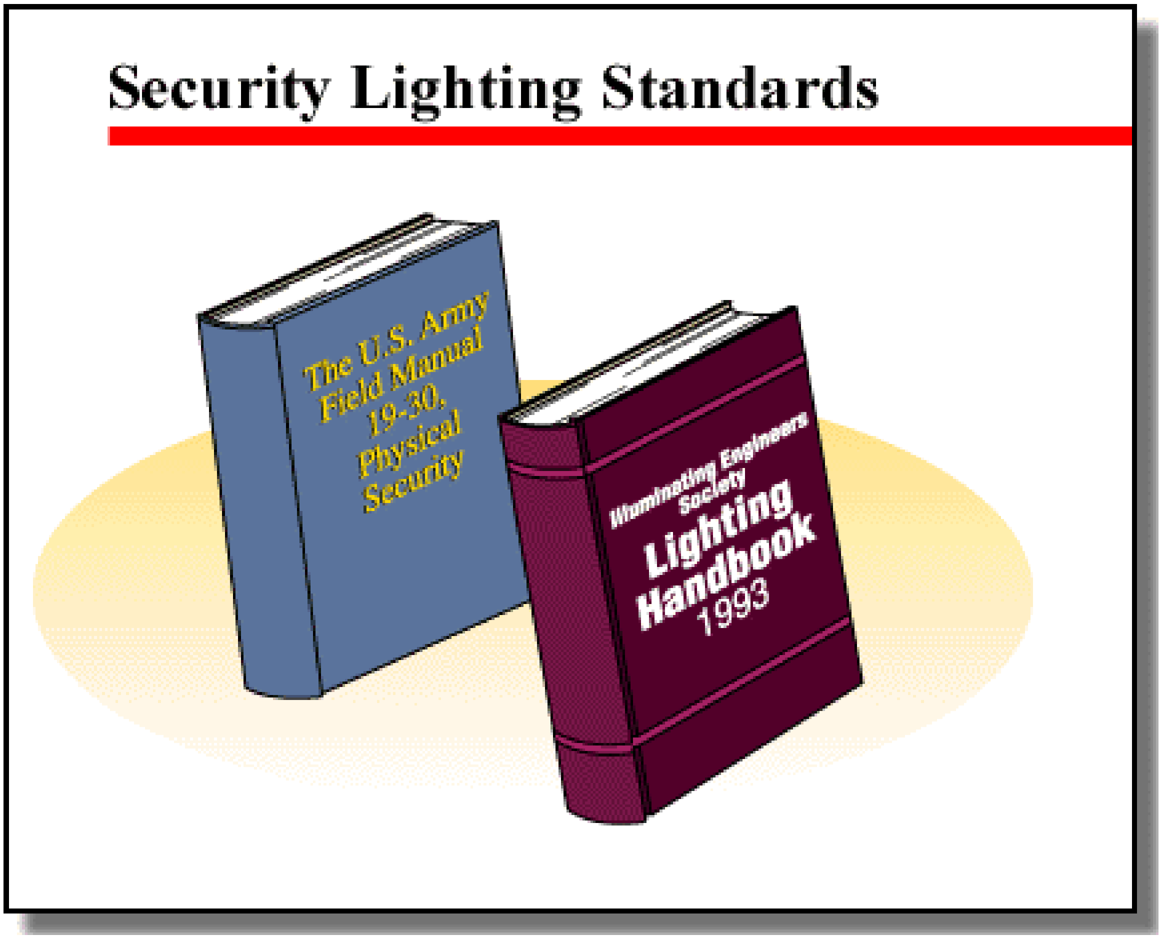
Designers of a protective lighting system may, in any given region (area of coverage) and circumstance, use lighting primarily as a psychological deterrent. Recall that lighting as a psychological deterrent creates in an intruder's mind the awareness that he or she will be discovered and observed during any unauthorized entry attempt. As a general rule, however, designers may view psychological deterrence more as an added benefit, given specific situations (in a design intended primarily for object illumination or physical deterrence). When lighting is used as a psychological deterrent, it is imperative that the lighting system be interfaced with CCTV, alarm systems and security response forces. This is essential in order to ensure maximum deterrent effect.



Lighting as a Psychological Deterrent

Security Lighting Standards

There is currently no U.S. national standard for protective or security lighting. In the absence of such a standard, many turn to The *U.S. Army Field Manual 19-30, Physical Security.* This manual has been used as a reference for protective or security lighting for many years. Another resource, the Illuminating Engineers Society (IES), *Lighting Handbook, 1993*, also serves as a reference for protective and security lighting. The third source of information on this subject is the Nuclear Regulatory Commission Physical Security Standards. This document provides in-depth discussions on isolation zones, protected areas, clear zones and other restricted areas requiring protective lighting. These three resources [provide essential information; nevertheless, they also do not always agree. You can, for example, get three different lighting recommendations for a given area, which can result in confusion at a minimum and unnecessary expense at worst. The solution to this situation is for designers to perform a comprehensive Vulnerability Assessment. Then, building on that assessment, designers must perform careful analysis to determine the true requirements of an area to be illuminated. The appropriate level o lighting will then emerge as the planners design a system that meets their intended objectives.



Security Lighting Standards

The U.S. Army Field Manual 19-30, Physical Security
Illuminating Engineers Society
Lighting Handbook 1993

Lighting Application Issues

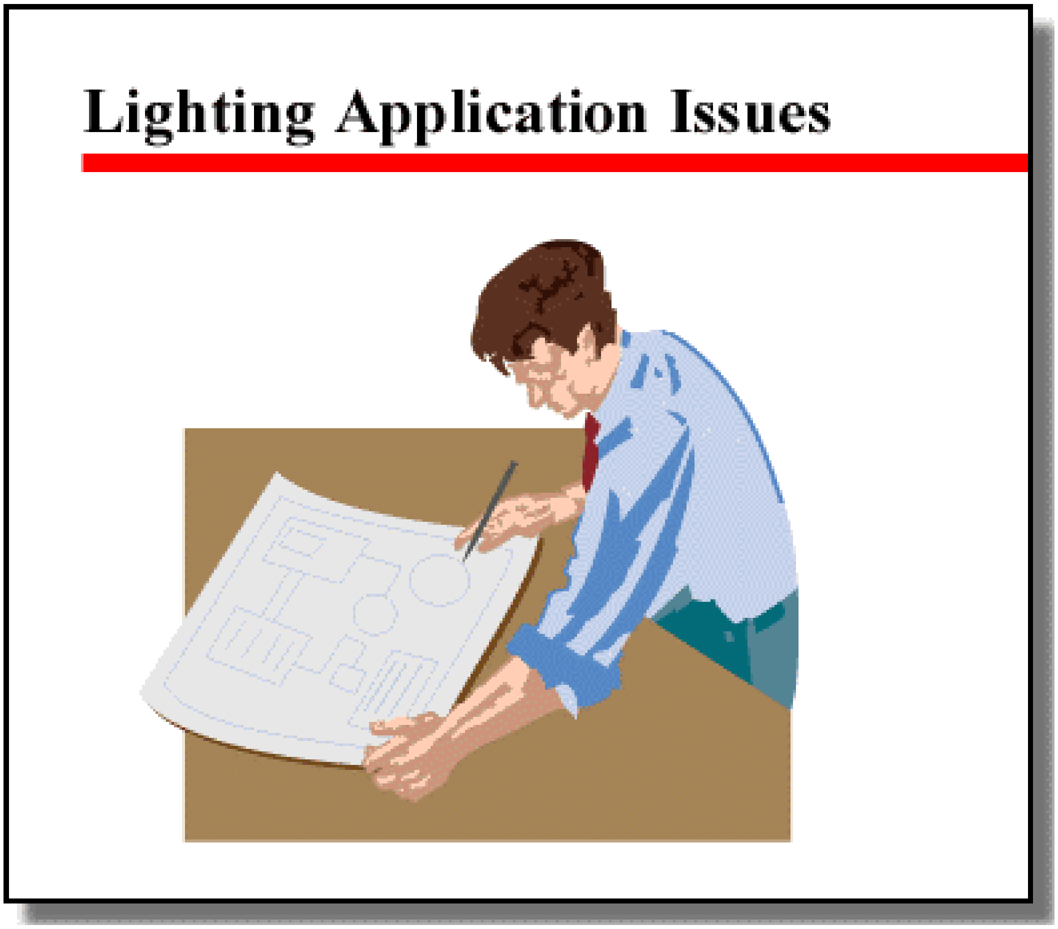
Select the first topic below to begin this lesson:

TOP

Application Issues

It should be apparent from the discussions in the preceding pages that lighting requirements vary according to each security application (object illumination, physical deterrence, psychological deterrence). All of these applications have different requirements for intensity, distribution, quality, sources and reliability. In addition, appropriate lighting for a given area is affected not just be the requirements of the security plan for the area, but by conditions in the surrounding areas as well. For example, a designer's plan for protective lighting must account for the impact lighting from an adjacent property, especially if there is resulting glare.

In the following sections, we will focus on illumination intensity and quality in more detail.



Lighting Application Issues

Light Intensity for Object/Area Illumination - Design Issues

With object illumination, the goal is to provide sufficient light over the area to detect anyone moving in or around the area. At the same time, lighting systems should whenever possible limit the intruder's view of the area. This strategy is intended to impair the intruder's ability to ascertain whether they are under observation.

An effective security lighting system for object illumination should:

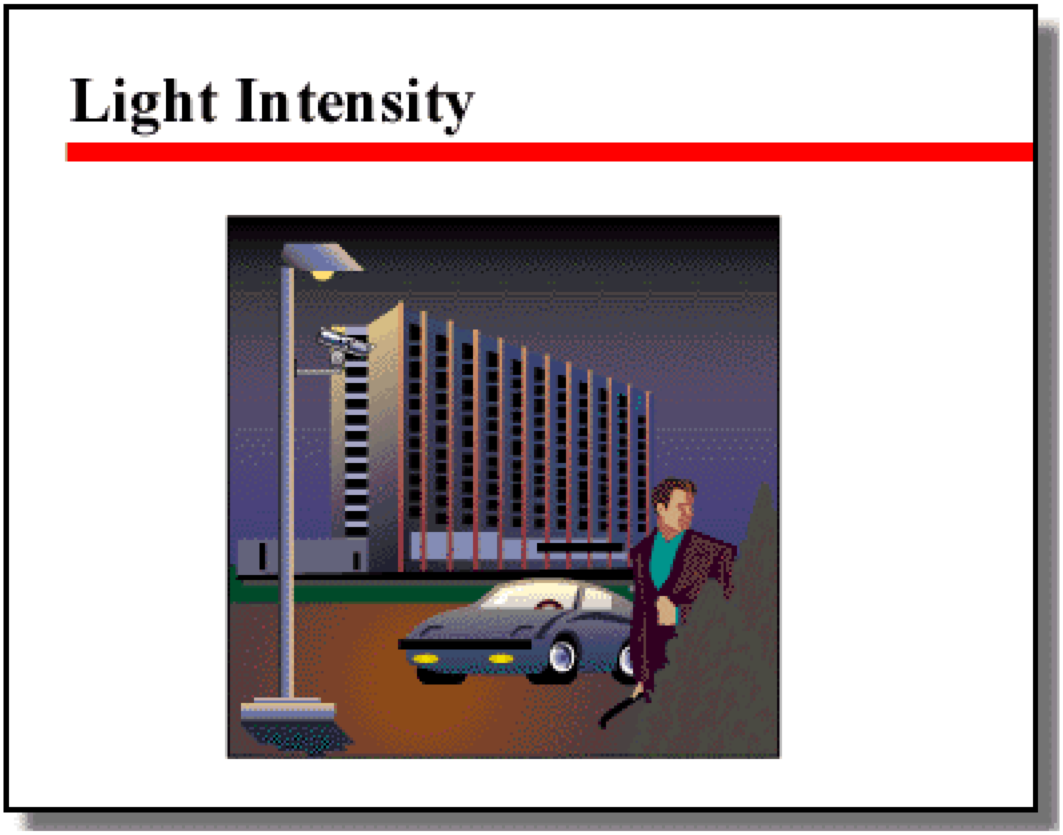
- discourage intruders
- make detection of attempted entry highly probable
- avoid glare that annoys neighbors, workers, security officers or passing traffic
- provide adequate illumination whether the surveillance is by electronics or the human eye
- render the observance of security posts, CCTV cameras or other electronic sensors by intruders to an imperceptible level
- provide for special treatment of entrances, exits and other sensitive locations.

Further, such a lighting system must be designed with careful attention to several additional factors that impact on its overall efficiency. System designers should:

- provide reliability through redundancy of components
- provide for easy control and maintenance
- determine the required illumination by viewing the scene under varying natural light conditions
- determine the distance between the surveillance element (person, camera) and each element of the illuminated object or scene

- determine the purpose of the observation: recognition, identification or detection.

Each of these factors is a crucial design element which, when applied properly to the overall lighting plan, will yield a highly effective and efficient protection capability.

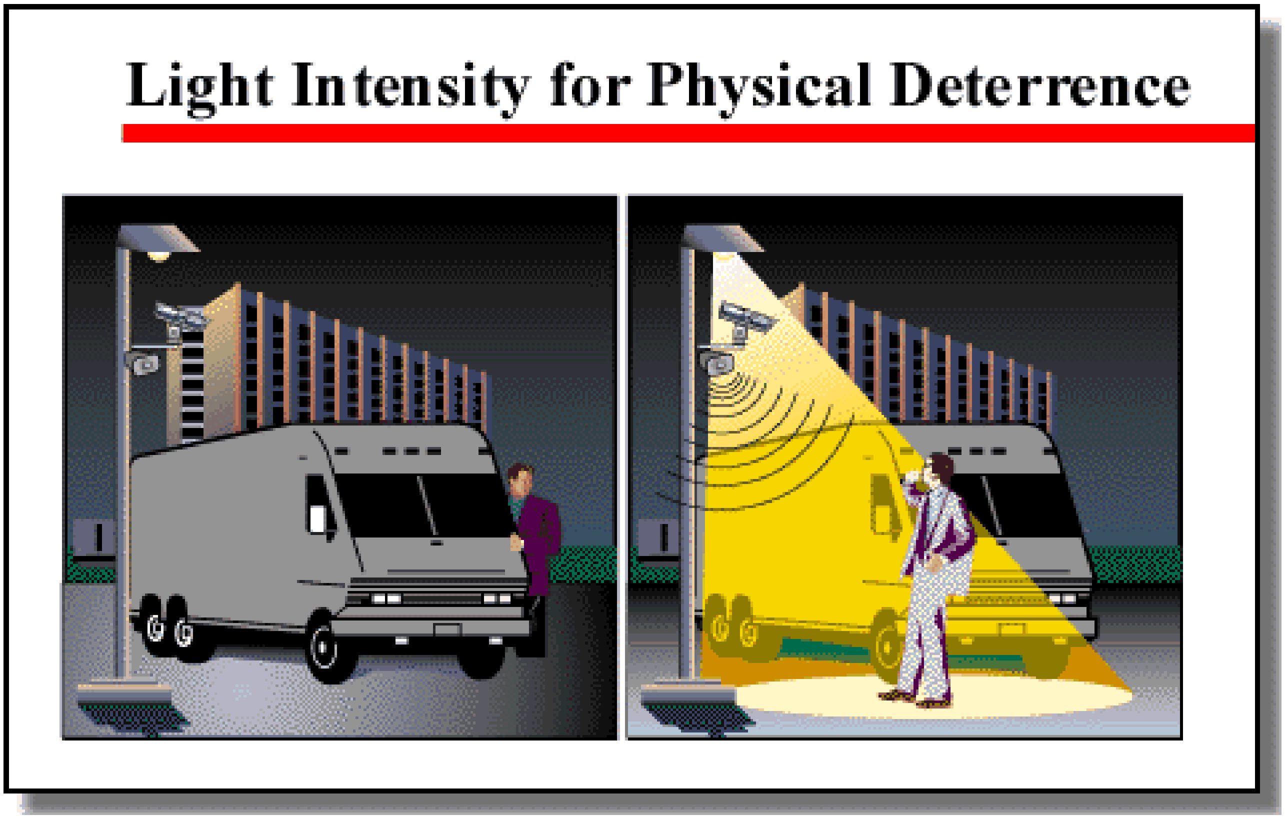


Light Intensity

Light Intensity for Physical Deterrence - Design Issues

Lighting intended to provide physical deterrence must use lighting intensity as a method to disable an intruder. The general design principle for physical deterrence lighting is use a level of intensity as low as possible to accomplish the desired effect. An effective lighting system for physical deterrence should:

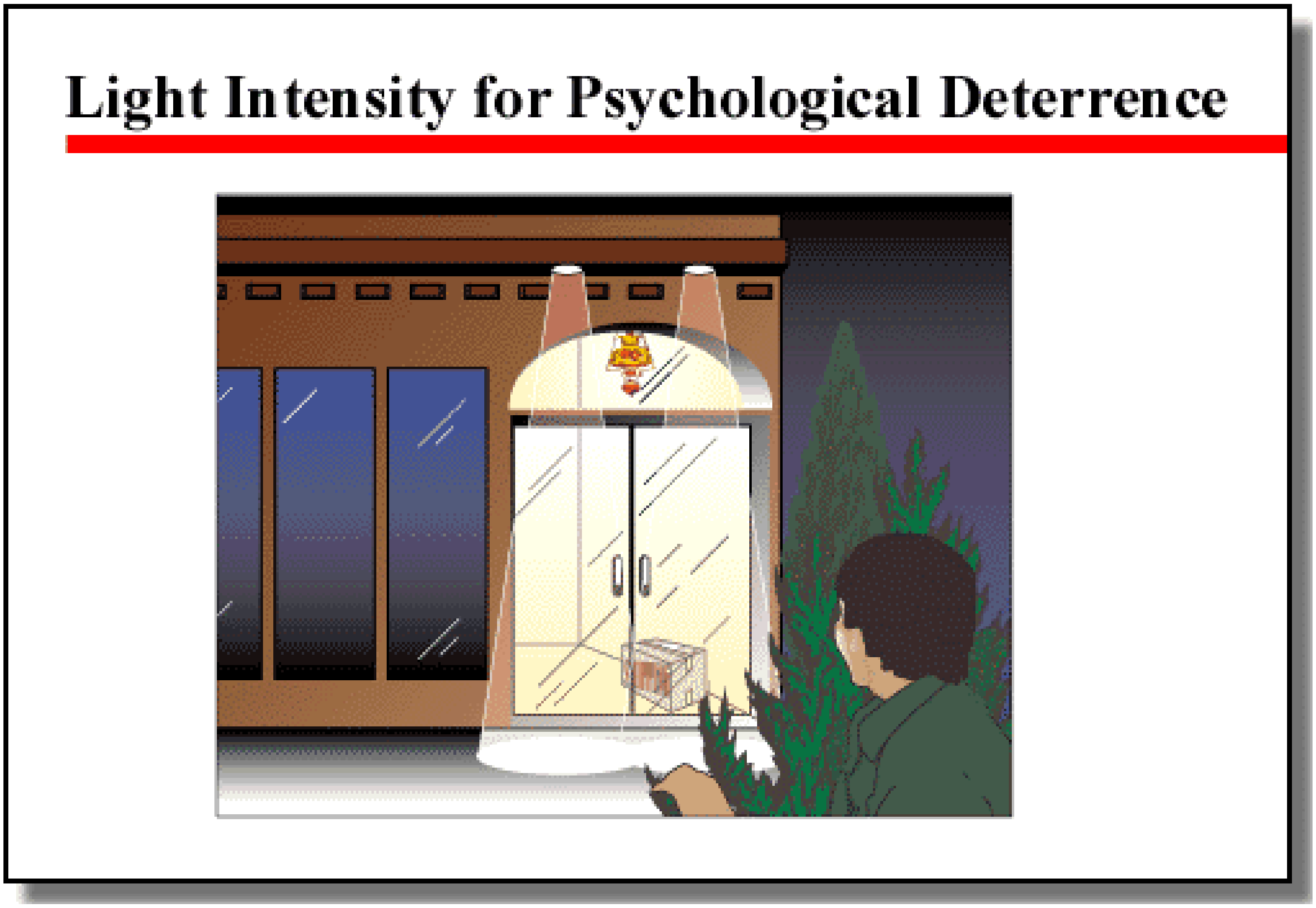
- Cause an inability to see normally, preventing further penetration of the area
- Cause specific physiological reactions to the light such as pain or tearing and change in ocular muscle stress.
- Cause temporary blinding which will vary in duration depending upon the intensity and character of the light source. Strobing of the light depending on its intensity and speed can cause prolonged disability to a person. The utilization of strobing light must include a legal review to determine what liabilities my be incurred.



Light Intensity for Physical Deterrence

Light Intensity for Psychological Deterrence - Design Issues

Remember that psychological deterrence is an intruder's belief and/or perception (perhaps accurate, perhaps not) that security at a specific location has diminished his or her ability to overcome the security measures in place. Lighting, as previously mentioned, can be an important tool in creating a psychological deterrence. The objective for designers of such a lighting system is to provide illumination intensity sufficient to convince an intruder there is a high probability of detection, identification or apprehension.



Light Intensity for Psychological Deterrence

Types of Lamps

In casual conversation, lighting terms are often used imprecisely. These are two terms which are often used interchangeably; however, in discussing technical lighting issues, their correct usage is important to avoid confusion. These are:

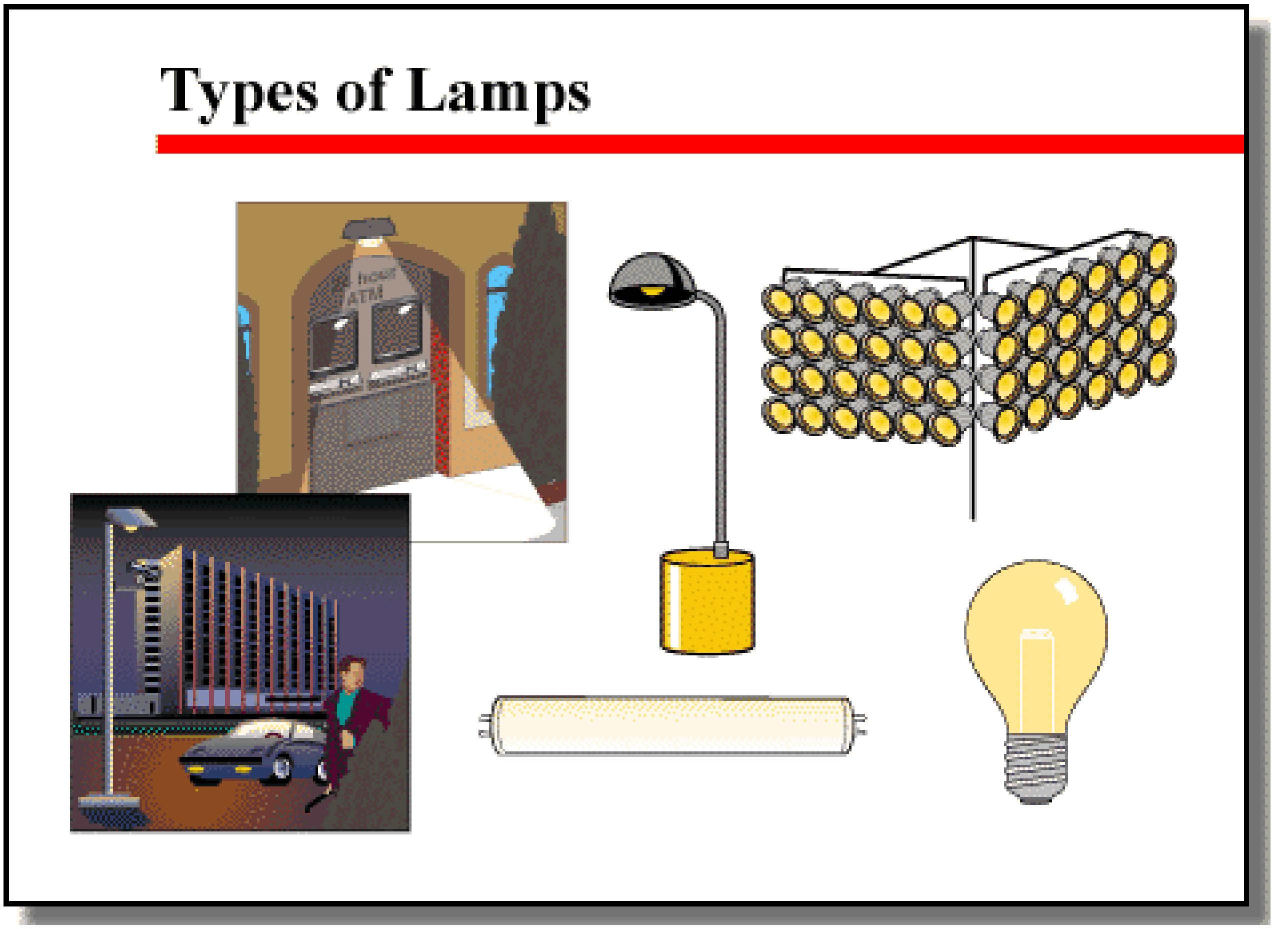
Lamp - the actual bulb or tube which emits light when electrical energy is applied.
Luminaire - the lamp, housing and all other hardware used in mounting and focusing illumination; also referred to as lighting unit, fixture, or instrument.

There are many different types of lamps used in modern protective lighting systems:

- incandescent
- fluorescent
- mercury vapor
- metal halide
- high pressure (H/P) sodium
- low pressure (L/P) sodium)

Each has its own unique characteristics which determine when the particular lighting is suited to a particular task. For example, low pressure sodium provides relatively high levels of illumination at low cost. Often they are used to light highways; however, L/P Sodium lamps tend to distort colors significantly. Using L/P sodium lighting for a parking lot at a car dealership, therefore, would be inadvisable, since customers would be unable to get a true representation of the color of the vehicle before them.

Mercury vapor, metal halide, and high-pressure sodium are known as high-intensity discharge (HID) lamps. These lamps provide the highest efficiency and longest service life of any lighting type. They are commonly used to outdoor lighting and in large indoor areas.

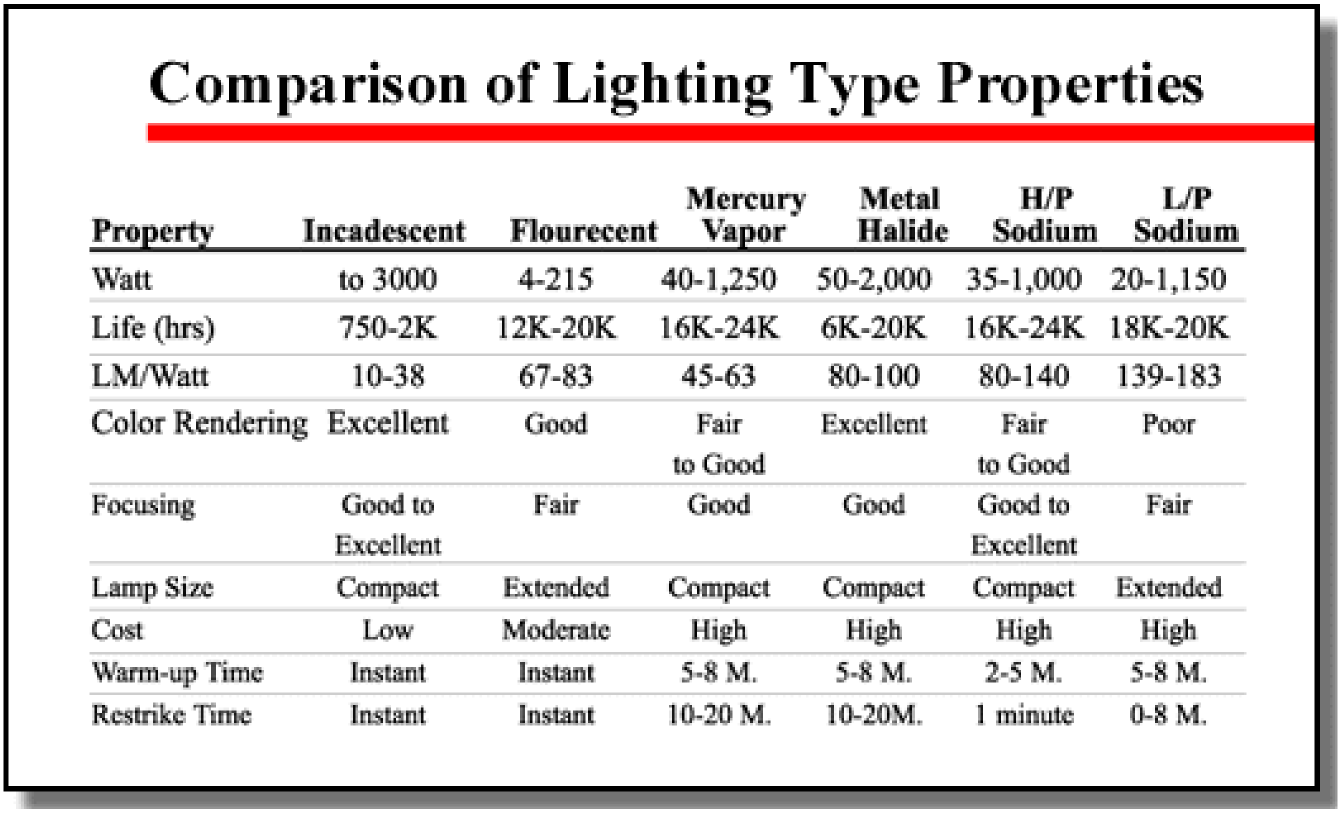

Types of Lamps

Illumination Quality

Factors to consider in selecting a lighting type are:

- the lumens per watt
- color rendering
- focusing capability
- warm-up time
- restrike time
- flicker rate

Illumination quality is the combination of all these individual factors. As in all security applications, determining the specific use for a system — in this case lighting — will define the resources required — in this case the illumination quality of the lighting system. Figure 2-24 above provides an overview of many of the factors effecting illumination quality. A discussion of several of these factors follows.



Comparison of Lighting Type Properties

Property	Incadescent	Flourecent	Mercury Vapor	Metal Halide	H/P Sodium	L/P Sodium
Watt	to 3000	4-215	40-1,250	50-2,000	35-1,000	20-1,150
Life (hrs)	750-2K	12K-20K	16K-24K	6K-20K	16K-24K	18K-20K
LM/Watt	10-38	67-83	45-63	80-100	80-140	139-183
Color Rendering	Excellent	Good	Fair to Good	Excellent	Fair to Good	Poor
Focusing	Good to Excellent	Fair	Good	Good	Good to Excellent	Fair
Lamp Size	Compact	Extended	Compact	Compact	Compact	Extended
Cost	Low	Moderate	High	High	High	High
Warm-up Time	Instant	Instant	5-8 M.	5-8 M.	2-5 M.	5-8 M.
Restrike Time	Instant	Instant	10-20 M.	10-20M.	1 minute	0-8 M.

Lumens per watt

Lumens is a measure of illumination. *Lumens per watt* is a measure of efficiency. It is the ratio of illumination to electrical energy used by the lamp to create the illumination. Lumen (LM) per watt have significant impact on the cost-effectiveness of the system.

Lumens is a measure of illumination. Lumens per watt is a measure of efficiency. It is the ratio of illumination to electrical energy used by the lamp to create the illumination. Lumen (LM) per watt have significant impact on the cost-effectiveness of the system.

Color Rendering

Color rendering is an important consideration if actual scene element colors must be observed or color CCTV cameras are to be used to record the scene. In such situations, it is important that natural colors not be distorted.

Focusing

Focusing is a luminaire's "spread;" that is, does it cover a wide area with diffuse light, or can it be aimed in a narrow beam of intense light on a small area. The intended use for a given lighting unit (object illumination: physical deterrence, etc.) defines the type of lighting unit required: wide or narrow focus.

Warm-up Time

Warm-up time is extremely important if maximum luminance is instantly required at the time of activation. Compare the values in the table on the previous page. Note that some types of lighting require as much as eight minutes to achieve their optimum output level. In some security operations, that would present an unacceptable risk.

Restrike Time

Restrike time is the period of time between a lamp's shut-down and its restart. Some lamps can be restarted immediately; others must "rest" for as much as 20 minutes before "restriking." Along with warm-up time, restrike time is critical to systems used to protect persons or high property value items, since such security systems cannot afford to be without sufficient illumination for extended periods of time. Thus, the amount of time needed to restore the system determines its value to the overall security program. If instant restrike is required, system designers must include a capability for an automatic restart stand-by system.

Flicker Some lamps have as part of their characteristics varying degrees of *flicker*. This may be most visible in the video produced by a CCTV camera using certain lamps as a source of illumination. It appears as "jumps" or rapid pulsing in the video. Flicker is a result of the alternating current which supplies electrical power to the lamp. Some types of lamps are more susceptible to flicker than others. In addition to affecting video image quality, flicker rate has a more subtle effect. Individuals exposed to flicker for long periods of time — while perhaps consciously unaware of the phenomenon — can develop stress, and elevated levels of stress has a negative impact on personnel both at the psycho-social level and in terms of productivity.

Future Protective Illumination Standards

As mentioned in an earlier section, one comprehensive U.S. standard for protective lighting does not currently exist. Establishing such a standard would be extremely beneficial for designers of protective lighting systems. Any standard for protective lighting should include data clarifying:

- the positive correlation between the level of illumination intensity and the time required to detect an intruder or an exception situation