CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

Technical Guideline 9:
Security Engineering Design in Commercial and Institutional Facilities

Prepared by

Robert J. Haskell, Westinghouse Electric Corporation

June 1978

This project was supported by Contract No. J-LEAA-022-74 awarded by the Law Encorcement Assistance Administration, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Westinghouse Electric Corporation
Arlington, Virginia 22202

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

1. Introduction

Security engineering is the term used to describe the application of crime prevention strategies to the physical environment. These strategies result in changes to physical construction or spatial relationships as opposed to strategies designed to influence social organizations. The object of security engineering is to minimize or eliminate the opportunities for criminal behavior and, at the same time, to increase the risk, either real or apparent, to those who do commit criminal acts.

While security engineering strategies result in physical changes, their ultimate goal is to produce behavioral changes in people using the environment. Security engineering is, therefore, more than target hardening, that is, using locks and alarm systems to prevent entry by unauthorized personnel. Although it includes target-hardening measures, security engineering considers the complete physical environment and evaluates how each aspect contributes to, or detracts from, security. Therefore, in addition to physical design changes, it takes into consideration all elements of the facility including traffic flow, facility management, and support by local law enforcement agencies.

The guidelines presented in this document focus on the application of security engineering strategies at the planning and design stage. More options are available at this point, and those selected can be most easily implemented. Changes in spatial relationships and design can

be made at little or no additional cost. Applying such security measures after a facility is completed may entail more expenditure of funds and disruption of operations than is felt warranted. However, while this document focuses on the application of security engineering strategies at the planning and design stage the strategies described can be applied to a facility already constructed, with the understanding that additional costs will almost certainly be involved.

Because of the emphasis on the early implementation of security engineering strategies, these guidelines will prove most useful to architects and city or community planners. They will also be useful to anyone concerned with the construction or renovation of a facility or with security maintenance. They should be considered by those who make policy decisions concerning new construction, such as building inspection offices for a jurisdiction. In fact, building codes based on security engineering principles could very well be developed and made part of the requirements for municipal building projects, particularly for facilities (with special security problems (such as hospitals and courthouses).

Specific strategies are offered for three kinds of facilities: An individual building; a complex of buildings (e.g., a hospital); and an entire installation (e.g., an industrial site). These strategies are considered in terms of site planning, perimeter control, traffic and parking, building design, and shipping and receiving. Specific implementation suggestions are offered. A final section focuses on security measures that are most applicable for facilities being renovated.

2. Security Engineering Approach

Security engineering is based primarily on two concepts: Access control and surveillance. Limiting access to a facility is one of the best means of deterring criminal activity, as is keeping the potential offender under surveillance.

2.1 Access Control

Access control is primarily directed at decreasing exposure to criminal activities. In essence, it operates to keep persons out of a particular locale if they do not have legitimate reasons for being there. In its most elementary form access control can be achieved in individual dwelling units or commercial establishments by use of adequate locks, doors, and the like (i.e., the group of design strategies known as target hardening).

However, when one moves beyond private property to public or semi-public spaces, the application of access control becomes more complicated. Lobbies of apartments, office buildings, or schools are often open to the public and, consequently, to those persons who will commit offenses if the opportunity arises. One strategy is to station guards at entrance points to screen visitors, but this is both costly and potentially counterproductive if arbitrary decisions must be made.

Access control is most difficult to achieve on streets and similar areas that are entirely open to public use. In some areas, such as neighborhoods of tightly knit ethnic groups, the streets are effectively denied even to certain noncriminal outsiders by the imposition of social

barriers. However, there are other, more legitimate techniques for limiting access in areas nominally open to the public. Physical barriers imposed by natural forms (e.g., rivers and lakes), existing manmade forms (e.g., railroad tracks, parks, vegetation, highways, and cemeteries), and artificial forms designed expressly as impediments (e.g., street closings and fences) serve to restrict or channel movement and to limit access.

In facility design, the access control concept requires restricting the movement of personnel to the minimum necessary for legitimate purposes. Support facilities should be located near parking lots, shipping and receiving points should be consolidated, and routes to and from these areas should be as direct and short as possible. Outpatient facilities in a hospital should be near an entrance. All of these are examples of access control.

Because any strategy that fosters access control is also likely to impact upon egress, careful consideration should be given to access control strategies. They may not only limit the egress of offenders, but also hinder the mobility of potential victims.

2.2 Surveillance

Although similar to access control in some respects, the primary aim of surveillance is not to keep intruders out (although it may have that effect) but, rather, to keep them under observation. Surveillance increases the perceived risk to offenders, and the actual risk if the observers are willing to act when potentially threatening situations

develop, A distinction can be made between organized surveillance and natural or spontaneous surveillance.

2.2.1 Organized Surveillance

Organized surveillance is that which is provided by a dedicated source, such as a police patrol, in an attempt to project a sense of omnipresence (i.e., to convey to potential offenders the impression that police surveillance is highly likely at any given location). The effectiveness of this particular technique may vary greatly with geographic considerations, temporal and crime-specific factors, and the efficiency of the police themselves. There is some evidence that community/police cooperation may be increasing spontaneously, and the spread of such indicators might prove a potentially important trend.

Organized surveillance also can be achieved by nonhuman techniques such as closed-circuit television (CCTV) or alarms. Noteworthy success is reported to have been achieved in certain residential complexes where the CCTV surveillance channel can be dialed on residents' individual sets; this medium provides an additional window on the world and even serves to promote social interaction. Better results might be achieved if the surveillance function of the CCTV channel or channels were transformed or subordinated into one of several communications functions of the same system, so that crime surveillance could occur as a natural byproduct of a system actually serving several positive purposes.

Security engineering ensures that traffic routes and design of facilities support the use of patrols, and that provision is made for

electronic surveillance support during facility design or renovation. Basically, security engineering supports the use of organized surveillance.

2.2.2 Natural Surveillance

Natural surveillance is that provided by nonsecurity resources and can be achieved by a number of design techniques, such as channeling the flow of activity to put more observers near a potential crime area, or creating a greater observation capacity by installing windows, enclosing a staircase in glass, or using single-loaded corridors. Proper attention to the design concept can lead to a reduced number of conventional guard posts and greatly enhanced security. Relocating a bicycle rack so that it can be observed through a window by the bycyle owners in the normal course of their work is an application of this concept.

3. Security Engineering Strategies

Security engineering strategies are designed to minimize any criminal activity that can be influenced by environmental design. Included, therefore, is theft by nonprofessionals (employees and customers), as well as by professionals (intruders). These strategies are designed to minimize temptation and increase the risk of being observed rather than to accomplish total access denial. This approach is probably best illustrated by the following guidelines, which are applicable regardless of the situation being addressed.

- Parking lot location is a crucial element of pilferage control. Parking should be convenient, but routes to and from the lots must be under surveillance. Foot traffic to and from the lots should be restricted to a few designated entry points by the judicious use of fences or other barriers.
- Commercial and visitor parking and traffic flows should be separate from employee parking.
- The number of professionally manned guard posts can in some cases be reduced by placing secretaries, receptionists, etc., so that they maintain surveillance over entry and exit points.
- Unsupervised entry and exit points (doors) should be locked, eliminated if not required, or designed as emergency exits with alarms installed to signal their use.
- Shipping and receiving points and associated traffic should be separated, if possible.

- Fencing is sometimes counterproductive. It is less costly and often more effective to use open landscaped areas as long as the landscaping is planned so as not to provide hiding places or concealed routes of entry.
- Security design, hardware, and operational policies are cheaper and often more effective than guard posts and fences (one 24-hour guard post requires 4 1/2 men at a cost of $50,000 to $100,000 per year). Design and hardware expenditures are a one-time cost.
- Early coordination with local law enforcement officials is required to obtain cooperation and help in designing site security.
- Vehicle movement should be limited by the use of artifical (but natural) barriers (e.g., trees, bushes, mounds).
- Areas around buildings should be clear for about 100 feet to enhance surveillance.
- Wiring and spare conduits should be sufficient to support the maximum need for security hardware foreseen for the life of the building.

- Where attempts at forcible entry through exterior walls are likely, building construction should be of tilt slab or other attack resistant construction, not cinder block.
- When designing the facility, high-value, sensitive, and pilferable item locations should be identified and so located as to inhibit loss (e.g., food, beverages, clothes, drugs, firearms).
- Facility management and security personnel must participate in security engineering, be trained in security principles, and assist by developing and implementing complementary operational procedures.
- Security engineering should consider three successive barriers to penetration:
  - The perimeter and structure relationship.
  - The building perimeter (lights, surveillance, construction).
  - Internal security and sensitive item location.

- A thief needs knowledge, time to plan, the necessary equipment, and an opportunity to work undetected. Denial of any of these will reduce or stop losses. Security engineering requires consideration of how best to deny each.
- Quality hardware and construction pay. It makes no sense to install an elaborate security system around a particle board door with a cheap lock or to install a good door and lock in a sheet-rock or other type of easily penetrated wall.
- to be effective, security must be implemented before construction starts and maintained thereafter (e.g., key control can be lost if keys are not controlled during construction).

No one strategy is likely to be fully effective by itself. Therefore, security engineering entails the incorporation of a family of complementary strategies. Just as employee parking lots should not be readily accessible to transients, neither visitor nor employee parking should provide access to vulnerable property. Convenience is an important consideration in the location of parking lots, but it is also important that lot location does not make theft convenient.

It has been said that most commercial loss is suffered at the hands of employees. It may be that a disproportionate portion of the security strategies are directed at the outside threat or, conversely, it may be that employees are assumed to be honest and loyal and, therefore, given insufficient attention as sources of loss. Whatever the reason, attention to deterrence of employee crime is often lacking. Again, the guiding principle is reduction of opportunity, and a mix of strategies is most effective. In short, the area should be the focus of concern, not the functional concept or strategy. As with the crime displacement theory, if only one strategy is implemented in an area, the criminal will simply bypass it and use an easier approach. When the area is used as the focus, many deterrents will be coordinated and no easy avoidance will be possible.

4. Security Engineering Applications

To be effective, security engineering strategies must be applied on as broad an area as possible. Ideally, strategies would be applied first at the installation level, then at the complex, and, finally, to the individual building. At each of these levels, the basic strategies would be similar but would have a different focus. For purposes of illustration, three representative areas are discussed in these guidelines: An industrial installation, a hospital complex, and a separate building. Additional applicatory examples could be developed for such areas as new towns, industrial parks, shopping malls, or residential neighborhoods.

4.1 Security Engineering for an Installation

The security planner for the installation should be concerned with influencing spatial relationships, perimeter control, and traffic flow plans. To do so,he must participate in the planning for the installation and be aware of the impact upon security of the decisions reached. He must identify the vulnerabilities of the installation, the operational characteristics of the functions to be performed, and carefully chart those activities and resources which will impact upon security. It is obvious that it is at this stage that proper security engineering can be most effectively (and inexpensively) incorporated. This is as true today as in 1971 when M. Liechenstein in his Design for Security wrote:

> " The key to economical security design lies in security planning before construction,.... and in sharing portions of the security system among other users.
>
> " The most obvious opportunity for multi-function usage is in providing fire, burglary, robbery, and utility protection, all of which have some commonality of goals, i.e., protection of property and/or personal safety."

4.1.1 Planning Considerations

4.1.1.1 Site Selection

Although it is not likely that security considerations will be the deciding factor in facility site selection, the security planner should become involved in the planning cycle as early as possible. If he can become involved at the site selection stage, it will provide him both an opportunity to point out security characteristics of sites being considered and to become familiar with the operations being planned. In the course of the selection process, he should discuss security with the other members of the team and indoctrinate them as to security concepts.

His security planning during this period should be at the detail level corresponding to that of other members of the team. However, it should include, at a minimum, considerations of natural barriers, both internal and external to the site, site access points, external traffic flow, the potential threat posed by surrounding communities, and the local crime prevention situation.

4.1.1.2 Site Planning

To successfully influence the site plan, the security planner must actively participate in the initial stages when the first functional grouping of activities occurs. In general terms, facilities utilized by distinct classes of personnel should be grouped, traffic from off-site should be routed to and from the facilities used by as short a route

as possible, and maximum use should be made of surveillance opportunities provided by facilities manned on a 24-hour basis. Specific strategies are discussed later, but following these general guidelines, shipping and receiving facilities would be grouped and sensitive material storage areas might be placed near an operation manned at all times (such as a fire station). Another consideration would be to group offices occupied only during normal duty hours so they could be easily patrolled and intruders would be conspicuous.

A possible approach is to prepare an occupancy and traffic flow plan showing conditions each four hours through the day. Use of such simple diagrams will serve to highlight traffic flow and surveillance problems, particularly if the locations of sensitive security items and operations are included. Some specific items to be considered are listed below.

4.1.1.2.1 Topography

The security engineer should make maximum use of existing conditions to enhance security and, where the natural or existent environment is to be modified, should ensure that security is enhanced not degraded. Open terrain improves visibility and surveillance; steep, rough terrain limits it. Both improved surveillance and access control can be achieved by grading, much of which will occur as a function of construction. Low mounds act as barriers and do not impede surveillance. Obstructions to visibility on or near the property, in the form of woods and undergrowth, may be either desirable or undesirable. Where woods

constitute a covered avenue of approach or hiding place, they should be cleared or contained by a manmade barrier. Where they are a barrier, the barrier can be enhanced by the use of fencing. A body of water, like an adjoining woods, is both a barrier and an avenue of approach to be considered in the plan. To the degree that it requires a readily observable crossing, a body of water is an excellent barrier. To the extent that the water is an avenue and a point of access, it is a weak link in the security chain. The security engineer should devise strategies to improve natural and formal surveillance and to restrict potential landing points if such access will pose a threat to his installation.

4.1.1.2.2 Perimeter Control

Some type of perimeter control is common to most installations. Depending upon the size and security requirements, this control may consist of commercial type fences, natural barriers, or elaborate barriers and associated sensors. The security planner should strive to make the maximum use of natural deterrents and to maintain a common level of security at all points. Specific external threats should be recognized by specifically developed deterrents. For example, an area adjacent to a school should be designed to either channel or prevent intrusion by children. Use of a barrier attractive to children, such as a woods or stream, should be avoided. Mounds of earth and low-growing, dense shrubbery would probably be effective. Barriers such as rivers, streams, ravines, buildings, and forests must be considered as avenues of approach as well as barriers and evaluated based upon

the degree of security desired.

4.1.1.2.3 Access

Access is a broad criterion applicable to the site, specialized areas, facilities, buildings, and activities within the site. The objective is to limit and control access within the limits imposed by authorized persons at authorized times. Good security engineering strategy will limit -- to the minimum consistent with efficient operation of the facility -- the number of points through which personnel and vehicles can enter. Flexibility is provided by including additional points of entry that are normally closed but can be opened for special purposes.

Access to specific areas (such as employment offices, medical facilities, and shops) is controlled by their location and traffic patterns within the installation. Access can be deliberately sacrificed to achieve greater surveillance. These kinds of judgments are made with the knowledge of the conditions of the time and place, recognizing that over the life of the installation those conditions and even the use to which the facility is put will change.

4.1.1.2.4. Traffic Control

Although sometimes construed to be a subset of access, the control, pattern, and flow of traffic is sufficiently important to security planning that it warrants separate discussion.

In the interest of efficiency, as well as security, the shortest, most direct route is the best. Long and circuitous routes increase

exposure and provide opportunities for on- and off-loading without detection. Therefore, the strategy is to lay out or change routes so that they are short, direct, and continuously under some form of surveillance.

Normally, pickup and delivery vehicles should be routed directly, by the shortest route, from the point of entry to the point of delivery or pickup. Moreover, access points, building arrangement, and road layout should be planned with this objective in mind. Minimizing points of entry and minimizing distances from point of entry to all destinations within the installation will require some design compromises.

4.1.1.2.5 Grouping of Facilities

Considerations relating to the arrangement of buildings, facilities, and activities within the installation are affected by the mission, size and shape of area, type of facility, number and size of buildings, and a myriad of other factors.

Parking facilities will be required at work, recreation, and housing facilities. Parking lots are vulnerable areas and should, therefore, be placed where surveillance exists in the normal course of activity in adjoining areas. Lighting and patrolling are added as required.

Deadend streets should be considered in housing and other areas to control traffic and limit access. Removable barricades can provide control to create deadend streets, as well as provide flexibility for exceptional traffic requirements.

Delivery and pickup sites are points whose vulnerability should be reduced by a combination of techniques, including short direct routes, physical separation, and planned surveillance. Scrap and salvage yards, trash pickup and deposit points, shipping and receiving functions, food delivery, and receipt of medical and other supplies not directly related to the principal mission of the installation are in the high vulnerability category. All are subject to the same strategies to minimize dispersion and opportunities for unobserved operations.

Open spaces between buildings and particularly between groups of buildings grouped by activity are needed to provide good fields of view, a sense of responsibility and proprietorship on the part of the users or occupants, and ease in identification of strangers arriving and departing. One hundred feet or more around major buildings is considered an absolute minimum.

4.1.1.2.6 Surveillance

The plan for surveillance should consider not only programmed and scheduled observation and inspection by guards and others having surveillance as an assigned function, but also intermittent informal surveillance. The formal portion of the surveillance plan provides manned gates, guard posts, and 24-hour coverage of critical areas (such as computer rooms, classified areas, and police stations). Although unscheduled, the informal portion of the plan is deliberately planned to ensure that vulnerable areas, property, and activity are within the clear view of persons directly related to the activity and

also others who may have no relation to (or responsibility for) it. The strategy for informal surveillance is to provide a field of view overlooking vulnerable areas and to ensure a minimum density of activity and personnel presence in the area during the most vulnerable period. There are numerous opportunities to substitute informal for formal surveillance without loss of effectiveness and at a cost saving.

Open spaces and spatial relationships -- as well as windows, walks, and other features that place people in position and able to observe -- are an integral part of the surveillance plan. Within an industrial installation, for example, a computer complex manned 24-hours a day could be located to enhance surveillance of a parking area, or an allnight cafeteria could be located so that its patrons would pass rooms or buildings where sensitive items were stored. Lighting required to illuminate walks and parking areas could serve a double function if it also illuminated vulnerable building entry points. In a similar fashion the location of windows to overlook a shipping dock makes possible observation of the dock by persons not working in the shipping department. In each case, the possibility of observation acts as a deterrent to criminal activity.

4.1.2 Specific Strategies

As in most real-world situations, designing for security at the installation level involves a series of compromises. The installation's primary purpose is to support accomplishment of a mission, or group of missions, and in some cases security considerations will be overridden.

In most cases, however, enhanced security can be achieved with no mission degradation, simply by manipulating spatial relationships or modifying facilities design. The major objective of the security planner is to achieve the latter at all times, and where security considerations conflict with other considerations, he should be prepared to support his recommendations with data on projected cost savings and enhanced security. Specific strategies that he should consider in developing his recommendations are noted below.

4.1.2.1 Perimeter Control

Security engineering can be viewed as the establishment of a series of deterrents to inhibit criminal activity. The first of this series is established at the perimeter, which should be viewed both as a means of limiting access and as a screening point. Security engineering recognizes that the majority of losses, dollarwise, are due to individuals who are authorized access to the area of loss. It also recognizes, however, that reducing opportunity by reducing exposure will reduce loss. The perimeter and its access points should be designed with both points in mind. Specific strategies that should be applied are to:

- Establish access points as close as possible to the areas to be served to minimize unnecessary travel on the installation. Access points servicing normal-hour functions only should then be closed during nonduty hours to simplify surveillance.

- Utilize low mounds and shrubbery to restrict installation entry and to enhance surveillance.
- Segregate commercial and normal traffic entry points to assist in shipping and receiving control.
- Provide nighttime illumination of boundary areas shining towards the exterior of the installation.
- Protect or secure openings such as culverts, tunnels, or ravines which could provide avenues of entry to the installation.
- Ensure that access points are well-lighted at night and that secured entrances are adequately equipped with locking devices.

4.1.2.2 Functions Grouping

Security is simplified if facilities having common security requirements are grouped. Residential areas, office buildings, repair facilities, and public support functions all have different types of users, different hours of use, and different types of security problems. By grouping them, common security procedures can be observed, and access and traffic patterns can be planned. Some specific strategies to enhance security at lower costs are to:

- Group office buildings or support facilities so that a minimum number of access points may be maintained during off-duty hours. Ideally, one security guard post could then suffice for two or more buildings.
- Place transient service facilities such as hospitals so as to minimize traffic flow through residential areas.
- Segregate commercial (e.g., shipping and receiving) facilities to enhance traffic segregation and control.
- Identify activities that operate on a 24-hour basis and position them to make use of the unpaid surveillance provided.
- Group and position any limited access facilities to minimize the area to be secured.

4.1.2.3 Parking Lots

The location and use of parking lots are critical to effective security since items stolen on an installation are traditionally removed by a vehicle. Detailed design of the parking lots may not be completed during installation design, but the security planner should ensure that their locations do not inhibit security measures. Strategies supportive of security are to:

- Use fences or other barriers to channel foot traffic to and from the lots through a few choke-points where observation of the types of material being carried by pedestrians to their cars can be observed.
- Place parking lots near the facility to be supported, but preferably in front of it so access routes can be observed by receptionists or other similar personnel. Parking lots should not be hidden in trees or other areas where surveillance is difficult.
- Provide parking lots for specific types of personnel or patrons of specific facilities.
- Select parking lot locations in conjunction with traffic flow design to minimize unnecessary travel.

4.1.2.4 Shipping and Receiving

The shipping and receiving functions constitute a point of contact by persons external to the operations, offer tempting targets at a vulnerable point in the line of control, and provide opportunities for collusion between persons internal and external to the operation.

To minimize vulnerability, a two-way point of control should be placed between both shipping and receiving and other elements of the operation. Shipping and receiving should be physically isolated from

each other, and external traffic should be routed to minimize access.

An example of a convenient shipping and receiving design is illustrated in Figure 1. Some of the features of this design which are supportive of criminal activity are:

- Shipping and receiving functions are performed on each end of a single large dock served by adjoining offices. It is possible to move material and products from shipping to receiving and vice versa at any point in either process. With or without collusion by plant personnel, a delivery truck driver can load items from the shipping dock with low risk of detection.
- There is no provision for surveillance of the shipping and receiving docks by plant personnel. Limited interior surveillance of functional areas is available through windows in the shipping and receiving offices.
- There are check points for vehicles entering and leaving the fenced plant complex, where documentation is timestamped in and out. Seldom is there a physical check of vehicles to compare payloads with weigh bills.
- It is relatively easy for a trucker who illegally loads material not consigned to him to leave the premises without detection.

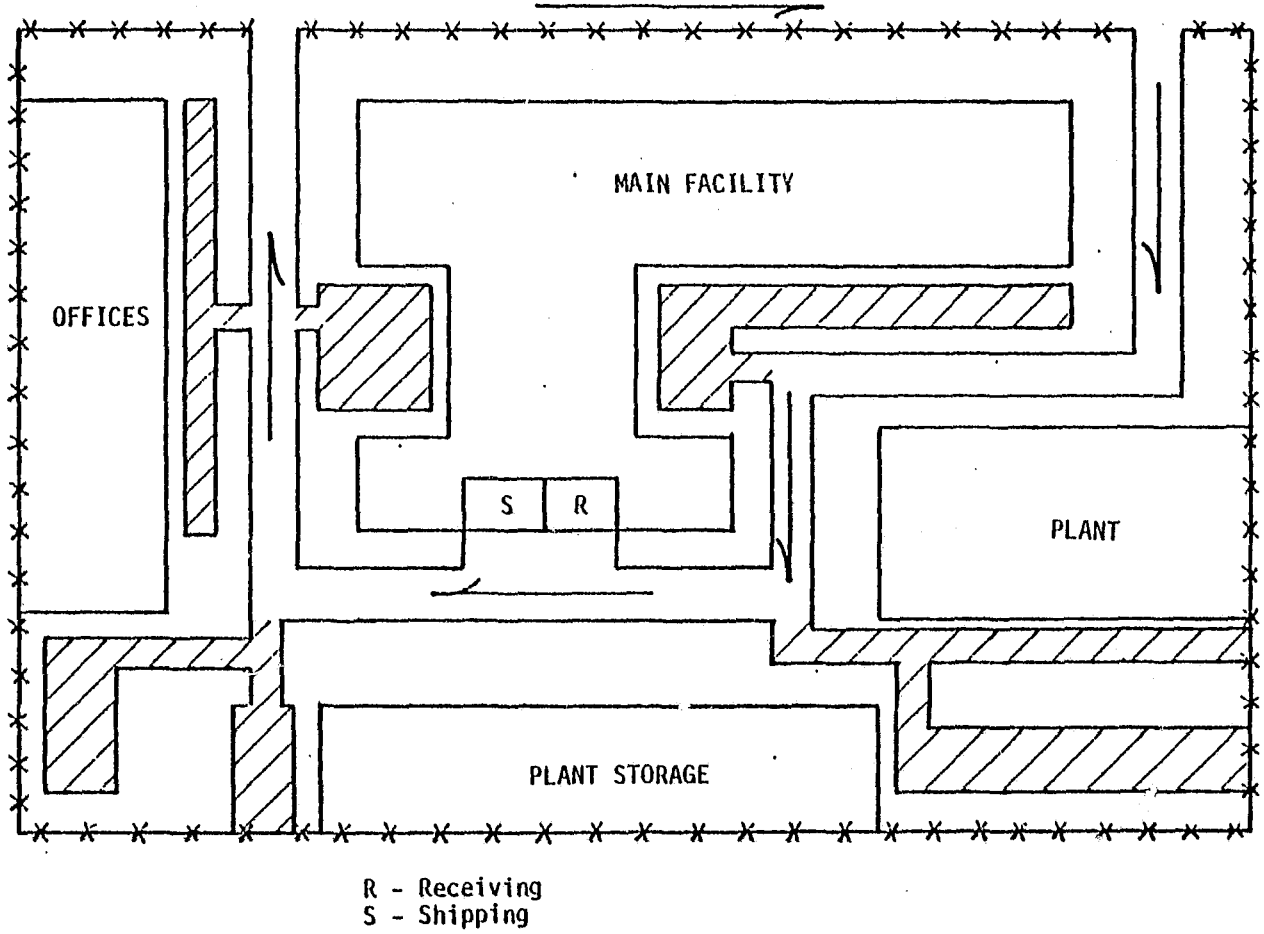


Figure 1. Poor Shipping and Receiving Design

- The location of shipping and receiving, relative to plant entrances, dictates a long and circuitous flow of traffic, several segments of which are not readily observed. The traffic pattern unduly exposes parking areas, increases the vulnerability of company property along the route, and offers the opportunity for truckers to stop in unobserved areas.
- The juxtaposition of shipping and receiving functions in a single open bay of the plant and adjoining undivided dock favors illegal movement of property from one area to the other.

A more acceptable design for shipping and receiving is shown in Figure 2. The major security engineering strategies illustrated are:

- Shipping and receiving functions are physically separated and correspond to, and enhance, flow of materials into, through, and out of the plant.
- A truck must physically move and make a separate approach for a pickup or delivery -- reducing the possibility of not dispensing a scheduled delivery or of making an unscheduled pickup.
- Deliveries and pickups are made through different exits.

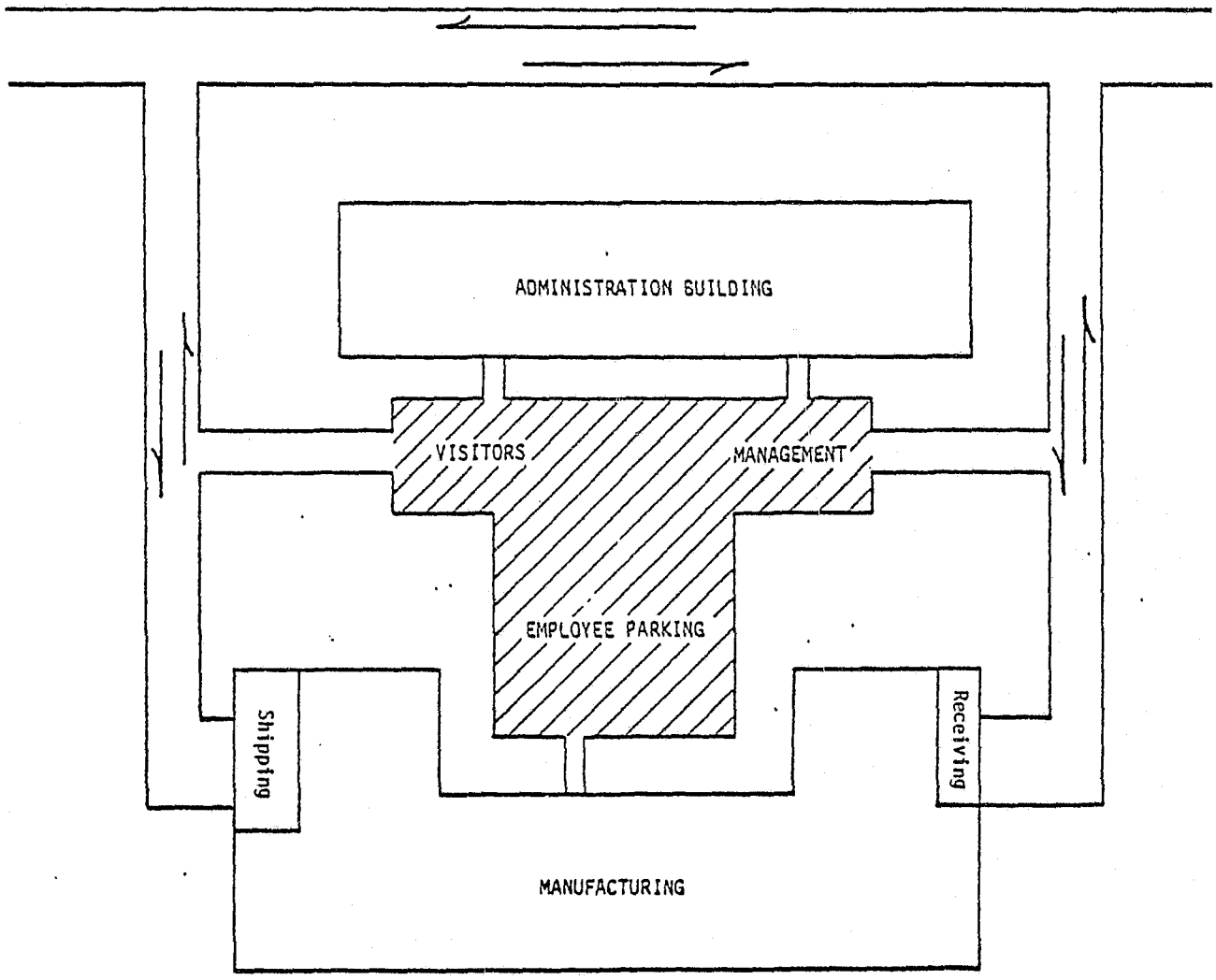


Figure 2. Good Shipping and Receiving Design

- The truck traffic pattern is short, direct, and does not expose other elements of the plant.
- Although there are no security guard check points to control entrance and exit, the docks and internal bays are designed to provide maximum surveillance.
- The internal shipping and receiving bays are physically isolated from the plant bays by attractive but effective barriers with convenient but readily controlled apertures (e.g., counters, gates, and doors).

4.2 Security Engineering for a Large Complex

Security engineering for the large complex parallels closely that for an installation. The planner must identify the vulnerabilities of the complex and relate these to the environment in which it exists. The difference is in scale. Where the planner for the installation can consider gross traffic flow characteristics, the planner for the complex should locate bicycle racks and management parking spaces.

The specific factors to be considered are dependent upon the operational requirements of the complex being planned. The complex used to illustrate the factors to be considered for this discussion is a hospital, since it presents many opportunities for the application of security engineering techniques.

4.2.1 Planning Considerations

4.2.1.1 Site Planning

Although the location of the complex will normally not be influenced by security considerations, a security planner should be involved in site planning discussions at the earliest possible stages. The proper placement of particular functional areas in a complex is a major factor in achieving a successful security program. In developing the site plan, the security planner should identify the activities to be carried out in each building and should trace the traffic flow required to support each function at various times of the day and night. Vulnerabilities should be assigned, and sensitive items and areas identified. Consideration should be given to closing as many access points as possible during times of decreased activity, and to making the maximum use -- for surveillance -- of activities manned on a 24-hour basis. Other specific engineering considerations are noted below.

4.2.1.1.1 Traffic Control

The traffic control pattern is one of the major elements for consideration in development of the site plan. It includes location of parking areas, direction of traffic flow, and defining access and exit points. The objectives are to: Limit traffic to as few areas as possible so as to minimize opportunities for removal of hospital property; plan parking areas as close as possible to building entry points, while maintaining surveillance; and segregate the types of traffic. If numerous entry points are necessary during the day or operational time period, consideration should be given to the closing

of certain of these points during the evening or nonoperational time period. Restricted entry and exit points render it more difficult for a malefactor to escape, and the security force can be more effective as their activity of concentrated surveillance, along with high visibility, can be maximized. Specific attention should be given to how the traffic flow and parking facilities will appear during times of limited operations. For example, nurses working in the early hours of the morning should be provided with parking that is under surveillance of either a guard post or a station manned 24 hours per day. An example of how parking can be planned to make use of surveillance provided by a security guard post, and to accommodate different types of traffic, is shown in Figure 3.

4.2.1.1.2 Building Locations

The placement of buildings, parking areas, and building entry and exit points are directly related and require careful correlation. Building locations should provide a clear area between the site perimeter and the building for surveillance. In some cases, the building must be located along the property line and so must provide an element of perimeter protection. In the case of multiple buildings situated close to the property line, a fence or wall connecting the buildings can serve as a good perimeter control, depending on the number and location of building openings. Use of buildings as part of the perimeter security can, however, be detrimental to security and should be avoided if sufficient space is available. If buildings are so used, careful attention must be paid to reducing their vulnerability to intrusion or egress. Walls should be sheer, with no convenient handholds for in-

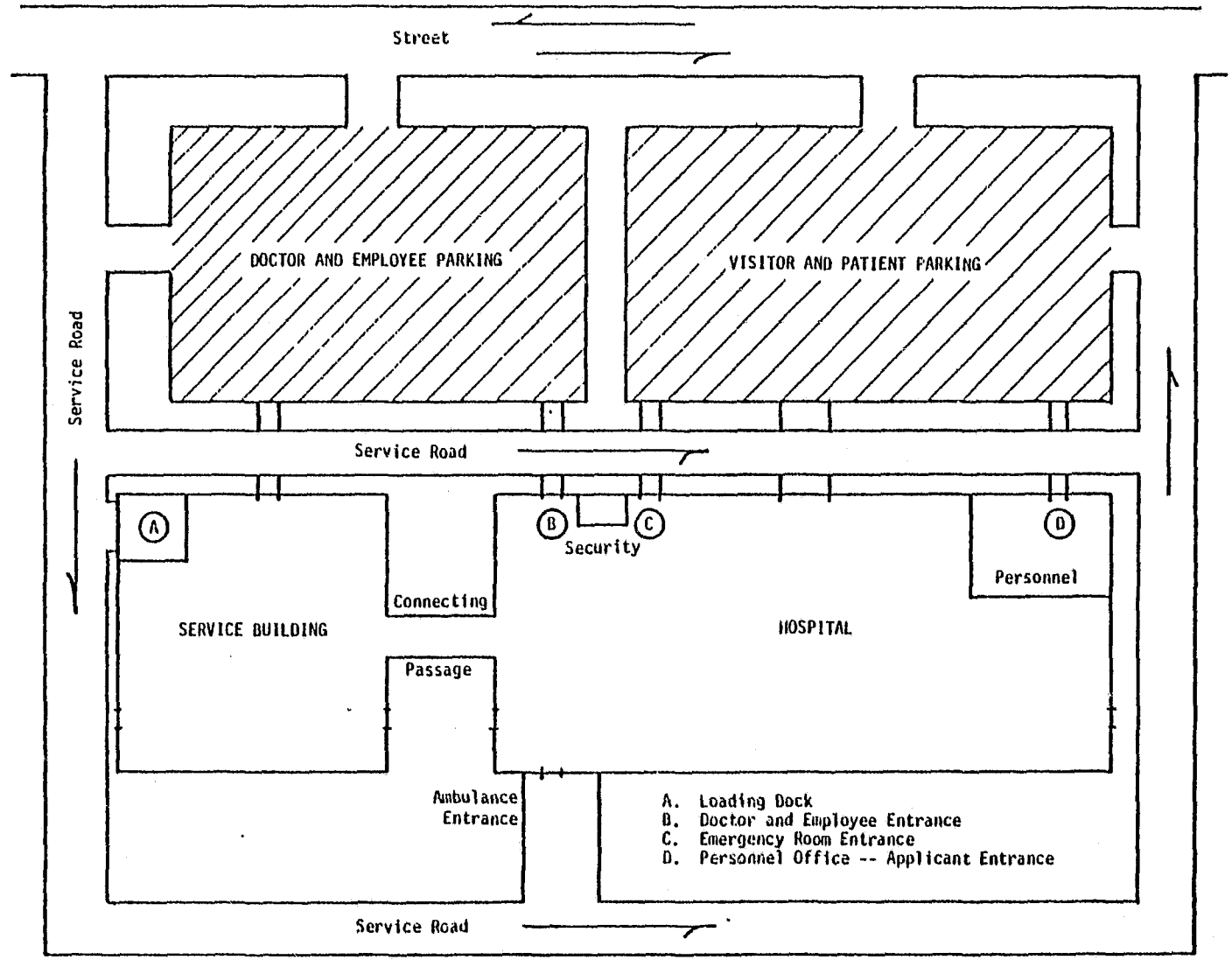


Figure 3. A Parking and Traffic Pattern Plan

truders, and windows should be eliminated or permanently closed.

Building placement is important in avoiding vulnerabilities. For example, in one complex of many buildings, patient care units were scattered throughout the site. A particular problem in this regard was the all-night delivery of emergency drugs from the main pharmacy to these fairly distant buildings. Not only was a vulnerability created for a drug robbery but for an assult as well.

If the security planner had evaluated traffic flow (which includes pedestrians) for the entire 24-hour period, he would have been able to recommend that these facilities be grouped and placed closer to the pharmacy.

During the considerations of building locations, various alternatives should be evaluated, with maximum use made of opportunities for unpaid surveillance (i.e., if a facility is operational 24 hours per day with patients or workers coming and going,they can serve as unpaid assistants to the security force). In short, every effort should be made to make the physical complex complement the normal operational procedures to produce enhanced security.

4.2.2 Specific Strategies

Some of the many strategies to be employed in designing for security are noted below. Their application is a matter of judgment and must be based upon the actual situation, since individual strategies often conflict with one another. For example, delineation of access limits calls for the use of bushes, trees, or mounds, while surveillance

would call for a completely open area. Thus, the resulting plan must achieve a compromise. Low bushes, different surfaces, or plantings are used to achieve the maximum security consistent with the situation. Fences have been cited as being counterproductive, but they are often required to clearly define the limits of public egress and for safety. The competent security planner will mix his strategies to achieve his objectives.

4.2.2.1 Building Openings

Building openings include not only the normally considered windows and doors but also ventilators, crawl spaces, utility tunnels, interior courtyards, and emergency exits. It has already been established that the fewer the access points, the easier it is to provide surveillance and security. Beyond this basic approach, specific strategies that can be applied are to:

- Designate entrances for employee use only, and limit these as much as possible both as to number and as to hours of operation. While these are operational matters, the locations and types of doors must be determined based upon anticipated use. Location of locker facilities, time clocks, and parking all are affected by the location of such access points.

4.2.2.2 Employment and Purchasing Offices

One of the basic premises of security engineering is that decreased exposure results in decreased loss. Therefore, limiting access of

facilities to specific categories of personnel only is recommended. Within the complex, positioning offices such as the civilian personnel employment office and the purchasing office away from the main facility is, therefore, advisable. Specific strategies to be employed are to:

- Position the employment office in a separate building with associated parking, if possible. If not, separate it from the facility using a separate entrance and locked doors.
- Separate the purchasing office from the facility, possibly colocating it with the employment office.
- Group functions not requiring access to the hospital complex together, particularly when they attract traffic different from that of the other buildings of the complex.

4.2.2.3 Outpatient Areas

The same basic principle applies to outpatient areas as to the employment office. To avoid unnecessary traffic, outpatient areas should not be located deep within the facility. It is often difficult to locate the outpatient area in a separate facility, since common laboratory, x-ray, physical therapy, and pharmacies may support both inpatient and outpatient needs. It is, however, possible to locate the outpatient areas close to an entrance. The location of the outpatient areas must be

considered when planning for traffic flow, parking areas, and access points. The security planners must be sensitive to these relationships and point out the implications of decisions made based upon operational requirements.

4.2.2.4 Trash Removal

The trash removal facilities provided can also serve as a convenient, and usually ignored, method of removing sizable quantities of hospital property undetected. The location and types of such facilities should be chosen as part of the security plans. Strategies to be used to stop unauthorized use are to:

- Place the containers far enough from the building so individuals using them can be observed.
- Locate receptacles in the view of an office or station manned 24 hours a day.
- Illuminate the area.

If outside laundry services are used, similar care should be provided in the heavy-traffic areas.

4.2.2.5 Lighting

Good lighting is an inexpensive method for increasing security. For best results, the area lighted should be under surveillance, but lighting will serve as a deterrent even if no active surveillance is maintained. Psychological studies show that individuals perpetrating crime in the hours of darkness have a psychological fear of light itself. Lighting always should be considered during the development of the complex plan especially in relation to parking access points and

and pedestrian corridors. Some specific strategies are to:

- Position lighting to enhance surveillance of parking areas, particularly those positions to be used late at night.
- Provide lighting of pedestrian corridors from parking areas to access points.
- Light areas where losses could occur, or which could provide convenient places to transfer stolen items (i.e., trash receptacles, any unlocked doors not under surveillance).
- Light authorized access points.

The following guides should be observed when designing lighting installations to minimize vandalism and maintain illumination levels:

- Use break resistant lenses.
- Illuminate parking lots, using 14-foot-minimum-height light poles.
- Illuminate buildings with fixtures mounted on 14-foot-minimum-height light poles.
- Have lighting directed at the facility when building is to be patrolled from exterior.
- Have lighting directed to illuminate grounds around the facility when building is to be patrolled from within.

- Use increased levels of illumination at potential points of access into buildings.
- Illuminate walkways with 14-foot-minimum-height lights.

4.2.2.6 Shipping and Receiving

The routing and handling of commercial traffic always deserves specific consideration. In a hospital, the items being received are often of high value and small bulk, as well as sensitive in nature (i.e., drugs). Shipped items are usually not so valuable nor as numerous. Therefore, separation of shipping and receiving points may not be practical. However, separation should be considered, for the colocation of these functions provides an ideal situation for pilferage and large-scale theft. Strategies applicable are to:

- Provide as short an access and egress route as possible.
- Separate commercial traffic from user and employee traffic.
- Position docks so shipments are separate from receiving points.
- Provide high intensity of illumination to ensure visibility.
- Locate shipping and receiving facilities where they are overlooked by offices occupied by management personnel.

4.3 Security Engineering for the Building

Security engineering for the individual building should consider the perimeter to control unauthorized entry, access points to channel and segregate types of traffic, interior design to enhance surveillance, and location of sensitive items or operations to maximize passive protection. As in other areas, security planning should be initiated as early in the design stage as possible, and provisions for security-related wiring and hardware should be incorporated at the initial stages.

The application of security engineering concepts, strategies, and standards will vary somewhat with individual building requirements, but the basics, discussed below, remain the same.

4.3.1 Planning Considerations

4.3.1.1 Building Design

Architectural sketches and diagrams of any building should be closely examined by the security planner. Many examples exist where buildings are so designed that a series of steps are provided to the roof by an ornamental facade, or where multiple access points are provided by ground height windows shielded from observation by plantings. Objections to such feature at the design stage will usually be effective where they may not be at a later stage of construction. Such deterrents to good security are readily identifiable -- if designs are examined for that purpose. Unless that responsibility is assigned, however, it may never be accomplished, and an obvious security hazard will be created during construction.

In addition to such exterior design features, the interior groupings of facilities, and locations of corridors, elevators, offices,

and sensitive item storage or operations must be examined. As a rule of thumb, the more visibility the better, and the creation of blind spots or areas not subject to routine surveillance should be avoided.

Proper design can also have a positive influence upon the ways a building is used. Proper use can be encouraged by providing appropriate facilities that: (a) By their general nature, will not attract antisocial user groups; (b) by their design, will preclude antisocial groups; and (c) incorporate counteroffensive elements or mechanisms to reduce criminal opportunities and/or improve response time of security personnel following an incident. These facilities might include areas such as: Public restrooms, vending areas, equipment areas, and routes of access or egress (i.e., elevators, garages, and corridors). These areas should be designed in ways that prevent or discourage use for counterproductive or dangerous purposes. Design considerations might include locating the facilities where they can be more easily monitored, sizing the facilities for optimum control and to discourage use for purposes other than those intended, and providing control devices to restrict use to only authorized persons (e.g., closed-circuit television cameras, communications equipment, alarm systems, and lighting fixtures that can be used to increase the surveillability of the facilities and improve response time of security personnel). Also, the security engineering considerations and strategies for a large complex apply to the individual building and its exterior and perimeter. Grounds should be free of rocks and other debris, trees and shrubs should not obscure observation, and bushes or shrubs should be used to channel pedestrian flow.

4.3.1.2 Access Control

Access to a building should be designed to facilitate surveillance, control, and segregation of traffic by function. Dependent upon the functions to be accomplished by the occupants, access points should be designated as either to be closed during nonduty hours, or to be subject to surveillance and control for all-hours entry. Alarms should be installed at closed access and exit points to alert a guard to their unauthorized use. When building guards are to be employed, guard stations should be so designed and located that one station can observe and control as many access points as possible.

4.3.1.3 Surveillance

With the ever increasing costs of manpower, maximum use must be made of the security provided by the normal occupants of the building. In many cases, this can best be accomplished by proper scheduling of activities such as by arranging for cleaning or maintenance personnel to be present during nonduty hours. The presence of such personnel in a facility during the hours when it is normally unoccupied serves as a deterrent to unauthorized entry. The security planner can also do his part by ensuring that the design and locations of offices, corridors, elevators, access points, and manned stations facilitate observation by and of their users. A secretary station permitting a view of the corridor outside through a glass partition enhances observation -- and identification -- of unauthorized visitors. Receptionist desks permitting a view of access points and elevator banks add an additional (unpaid) guard post during duty hours.

4.3.1.4 Sensitive Items or Operations

Where the use to which the building will be put is known, sensitive item storage or operations can be identified. Examples of sensitive item storage are drugs in a hospital complex, precious metals in an industrial operation, classified material in a military operation, or a computer or communications complex where access must be controlled. The facilities for these should be located to minimize traffic by unauthorized personnel and to provide maximum deterrence to covert access and egress. Location on a perimeter wall should be avoided. Natural surveillance should be enhanced by the location of access points wherever possible.

4.3.2 Specific Strategies

It is stating the obvious to point out that the greatest majority of thefts take place within a building and that most are crimes of opportunity committed by individuals authorized access to the facility. In spite of this, however, most security planning concentrates on keeping out unauthorized intruders. Security engineering strategies (and standards) include design to restrict unauthorized entry, and the security planner must certainly observe them. He should also, however, be fully cognizant of how the spatial relationship of the building interior can be planned to decrease the exposure of pilferable items or to increase the risk of detection. Nearly all of the concepts and strategies presented throughout this report are applicable, depending upon the type building being considered. Noted below are strategies having general applicability.

4.3.2.1 Building Openings

Building openings include doors, windows, skylights, crawl spaces, utility tunnels, emergency exits, and any other route of access not through a wall. It is obvious that the fewer the openings, the easier the task of surveillance and control. Strategies that can be used to increase security are to:

- Locate windows on the ground floor as high as possible above ground level, and design them to restrict entry.
- Place bars on the inside of windows or other openings where breaking the window will activate an alarm.
- Wire emergency exits and those to be closed during portions of the day so alarms will be activated if used.
- Position receptionist desks or guard posts so that access points, including elevators, are under surveillance.
- Design access points so that routes to and from them are under surveillance, preferably by management representatives.

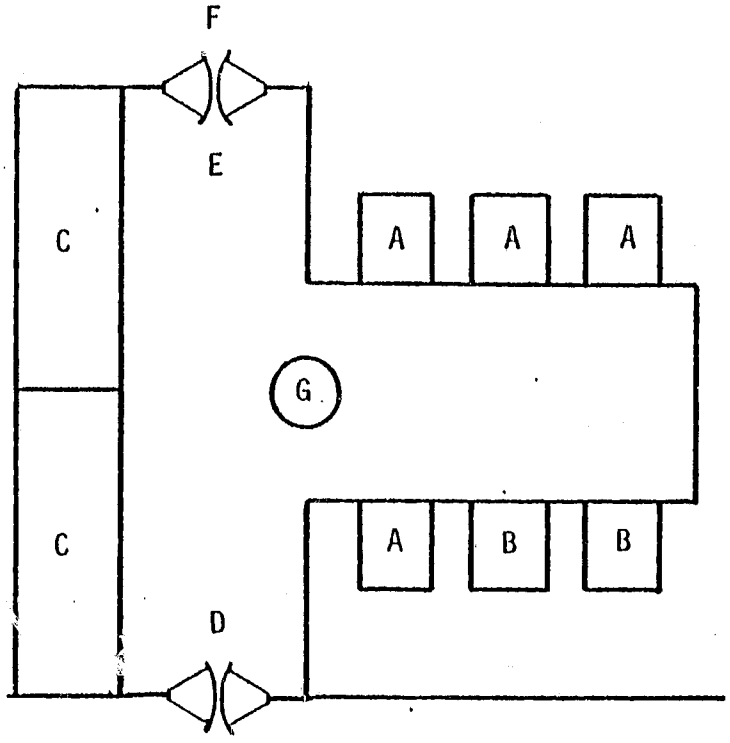
4.3.2.2 Elevators

Entry and exit routes to a building should be so designed that they can be monitored. This is particularly true of elevator banks servicing a garage or commercial area as well as an office or industrial complex. Strategies that can be employed are to:

- Program elevators so that separate elevators service the different sections of the building, requiring transfers at the ground floor within sight of a guard or receptionist.
- Design separate elevator banks with one servicing the garage or lower levels, the other the office complex.

Figure 4 shows the lobby arrangement of a building in which designated elevators are programmed to operate only between the lobby and parking levels; others operate between the lobby and the upper working levels. Therefore, persons entering the building from the parking level must exit the elevator at the lobby floor and, if proceeding to a higher level, board another elevator. The receptionist or security guard station is located so that the doors of all elevators, the building entrance, and lobby floor corridors are all in view. Persons entering the building from any access must pass this station; visitors, and employees during nonbusiness hours, must sign in and out. On request, escort is provided to persons proceeding to underground parking.

Figure 5 shows an example of how security can be frustrated by poor planning and design. In this design, while all elevators are programmed to make a short stop at the lobby floor en route up from the parking levels, they then proceed to the office floors above. The elevator banks at the lobby level can be accessed from any of three



A. Elevators serving lobby and specified floors above

B. Elevators serving lobby and floors below

C. Rest Rooms

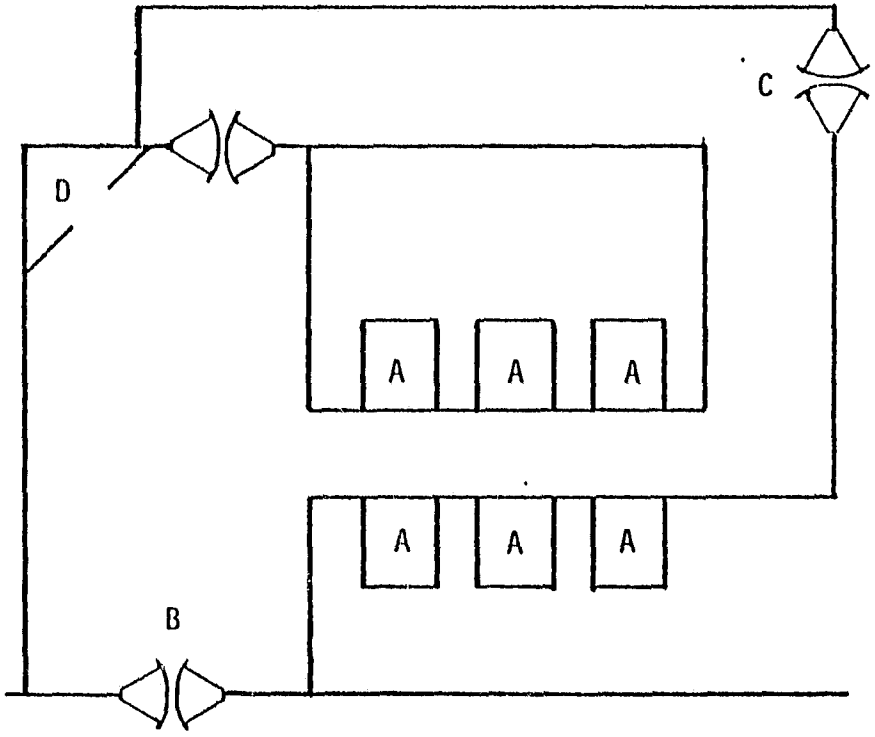
D. Building Main Entrance

E. Main Floor Corridor

F. Controlled access/egress door

G. Receptionist/Security Guard station

Figure 4. Effective Office Building Access Control



A. Through elevators from below ground to working floors

B. Main Entrance

C. Side Entrance

D. Guard booth

Figure 5. Ineffective Office Building Access Control

entries. The security station provides no visibility to the elevators and to only two of the three entrances. Moreover, the security station is not manned around the clock. Therefore, access to the lobby and upper floors can be gained from the parking levels and at least one lobby-level entrance at all times without benefit of surveillance; at times, all access is free of observation. Although offhours sign-in and sign out is specified and accommodated, it is not enforced. It is easier to leave unobserved than it is to enter because the elevators are not programmed to stop at the lobby on downward runs to the parking levels.

4.3.2.3 Surveillance

One of the best deterrents to crime is the knowledge that your act can be observed. Therefore, every effort should be made to incorporate design features permitting surveillance. Some effective strategies are to:

- Use open spaces whenever possible and avoid any design creating blind spots where criminal acts could be committed undetected.
- Eliminate columns and partitions that restrict vision.
- Use open space or glass partitions, doors, and windows around work stations to permit surveillance.
- Incorporate wiring for surveillance devices, such as closed-circuit TV, in building plans.

- Position any continuously manned operations so that their occupants will provide natural surveillance of critical areas.

4.3.2.4 Construction Considerations

In addition to the more generally applicable strategies noted, there are a number of security strategies that are applicable to building design. Some of these which should be observed or avoided are listed below.

4.3.2.4.1 Exterior Walls and Roofs

The following are conducive to security:

- Walls designed to prevent roof access.
- Flush, wall-mounted fixtures to deny handholds for climbing.
- Walls with a minimum of 12-foot height.

The following should be avoided:

- Decorative wall finish patterns and recesses for lighting fixtures that are climbable.
- Half-walls or free-standing walls connected to buildings.
- Recesses that provide concealment (e.g., recessed entrances, patios, accessible courtyards).
- Low, covered walkways.
- False wall fronts and/or wide roof overhangs.

4.3.2.4.2 Windows, Skylights, and Transoms

The following are conducive to security:

- Eliminate exterior window sills.
- Eliminate ground-floor windows.
- Use minimum number of windows.
- Use ceiling-level, horizontal strip windows (8-inch width maximum).
- Install window frames to place putty on the interior.

The following should be avoided:

- Skylights.
- Transoms on exterior door.
- Breakable glass in windows.
- Windows within 8 feet of ground level and 4 feet of doors.

4.3.2.4.3 Doors (Frames, Hardware, Locks and Keys, Openings)

The following are conducive to security:

- Minimum number of exterior doorways.
- Locks for elevator doors.
- One-inch minimum bolt length for all throw bolts used.
- Ceiling-to-floor zone gates for selected building usage after hours.
- Astragals on all double doors with panic hardware.

- Inside located, and lockable throw bolts for roof hatches.
- Nonremovable pins in door hinges.
- Key-operated locks with removable cores which can be changed after construction is complete if desired.
- Elimination of master-keyed locks, if and when possible, and strict control of a minimum number of master keys where it is not.
- Keys that require factory duplication.
- Exterior handle and lock access at main entrance only.
- Lockable slide bolts for overhead doors in addition to cylinder or padlock.
- Provision for securing operating shaft on crank-operated door as well as cylinder or padlock.
- Pry-proof metal door frames.

The following should be avoided:

- Surface-mounted locks.
- Locks having knob-mounted key access.
- Exterior doorways for restrooms that also open into interior of building.

- Doors to building exterior in
- secured storage areas.
- Recessed interior doorways.
- Doors on restrooms (use a maze instead).
- Windows in exterior doors.
- Sliding doors.

4.3.3 Additional Strategies

The following groups of design strategies are all important when considering the overall building design, with the primary intent being the reduction of destruction of property. A number of these also contribute to the concepts of access control and surveillance -- the primary means of inhibiting criminal offenders.

- Heating, air-conditioning, and ventilation units recessed in walls with locked covers flush with wall.
- Baffles for grills covering utility tunnels and vents.
- Strong grills on all utility tunnel openings, vents, and manholes.
- Key-controlled light fixtures in all public areas, with standard light controls for offices.
- Secured roof fans.
- Switches for exterior lighting located in secured areas, not hallways.

- Automatic controls for night lighting of corridors.
- Interior walls and ceilings:
  - Epoxy-coated, or equal, concrete or concrete block walls in restrooms.
  - Hard-glazed wainscoting on all walls.
  - Epoxy coating, or equal, throughout corridors.
  - Ceramic tile or block wainscoting on all corridor walls.
- Restrooms:
  - Heavy-duty fixtures.
  - Fireproof trash disposal containers.
  - Floor- and ceiling-mounted stall partitions.
  - Recessed shelves.
  - Burn- or scorch-proof commode seats.
  - Fewer restrooms with larger capacities each.
  - Hand-washing facilities located in hall alcoves, with minimal closed areas for commodes and/or urinals.
- Vaults and storage areas:
  - Solid reinforced walls to true ceiling height in all secured storage areas and vaults.

- Mechanical ventilation and no windows for secured storage areas.
- Secured storage areas located throughout buildings to provide safe storage for high-value equipment.

- Hallways, stairwells, and elevators:
  - Straight hallways.
  - No large enclosed stairwells.
  - Heavy-duty railings for stairwells.
  - Stainless steel elevator control buttons.
  - Elimination of all possible corridors.
  - Kickplate to the floor on stair risers.
- Mechanical and custodial rooms:
  - Machinery controls located in a single secured area with a locked control panel.
  - Custodial room large enough to provide secured storage for ladders.
  - Special paint locker secured against entry and located well away from main building.

The most important aspect in applying security engineering principles to any facility is to ensure their consideration at the planning stage.

Even if a strategy is not considered necessary for the initial uses forecast, but might be required later, it would be cost-effective to include as much of the strategy as possible (e.g., wiring for an alarm system without actually installing the equipment) rather than to have to renovate in the future.

4.4 Security Engineering during Renovation

Security engineering concepts and strategies applicable to the planning, design, and construction stages of a facility are also applicable to renovation of existing facilities. However, there are limitations on the concepts that are applicable at the renovation stage. Each change desired must be assessed in terms of practicality and cost effectiveness. For example, moving an entrance to improve access control might be advisable or might be neither practical nor cost-effective. The security planner is always constrained by cost considerations, and the least costly changes will be best received. On the positive side, loss data may be available, and the security planner is dealing with established procedures and a defined security plan. Therefore, he can design his strategies to counter known security problems.

Basic principles remain the same. The security planner should become involved in the renovation process as early as possible. He should become thoroughly familiar with the operational objectives desired and should, whenever practical, concentrate upon changes requiring relocations and refurbishing, rather than complete change. Although the security planner is somewhat constrained since he must accommodate his plan to an existing facility, it is in remodeling or renovation of

facilities that he will most often have a chance to enhance security. Therefore, security planners should take advantage of such occasions to upgrade protection and to progress towards their ultimate goals.

4.4.1 Security Master Plan

Every security planner responsible for a building, a complex, or an installation should have a master plan that details the improvements he desires to enhance security. With such a plan, every renovation project will provide an opportunity for implementing a portion of the plan. For example, alarm wiring can be included in new construction, newly added or modified doors can be positioned and constructed to improve security, new parking lots can have access and exit points redesigned, and lighting can be improved. Once a portion of the plan is implemented, securing the next portion is made easier. Examples of strategies for improvement that can be made at minimal cost, which are particularly applicable during renovation or remodeling, are presented in the following section. The plan should also identify existing features and structures whose demolition and removal could enhance facility security.

4.4.2 Renovation Strategies

4.4.2.1 General

Security engineering strategies easily accomplished during renovation or remodeling of existing facilities are noted below. They are drawn from actual strategies being implemented at CPTED demonstration sites.

4.4.2.2 Landscaping

Access control and surveillance can be enhanced by the proper use of landscaping techniques. Some applicable strategies are to:

- Use low bushes to delineate access routes, and public, semipublic, and private areas.
- Install additional lighting around parking lots, entrances, and secluded areas.
- Use mounds or ditches to restrict vehicular travel.

4.4.2.3 Parking

Parking areas are normally provided for vehicles and bicycles The security strategies applicable to both are similar. Some strategies to be applied are to:

- Place areas where the owners can observe them during their work periods.
- Restrict entry to any through vehicles by using deadends and restricted entry points.
- Restrict entry and exit points for pedestrians going to or from their vehicles to routes or points under surveillance.

4.4.2.4 Painting

Murals, graphic designs, and even different-colored paint can be used to distinguish between areas used for different purposes. If

individuals can distinguish those who are authorized in the area from those who are not, natural surveillance can be enhanced. Some strategies are to:

- Paint colored strips or walls to serve as guides between, or to differentiate, services or functions.
- Develop and paint wall designs to designate the functions being performed in the area.

4.4.2.5 Surveillance

Increased surveillance can be achieved during renovation through the judicious use of materials, redesign of corridors or stairwells, and repositioning of desks. Strategies that can be applied are to:

- Station secretaries' desks to face corridors, and use glass windows, glass doors, or open spaces to facilitate surveillance.
- Block off unused or dead space that cannot be readily observed (e.g., under stairwells, crawl spaces).
- Elininate bends or jogs in corridors.
- Move stations manned 24 hours to permit better surveillance of the facility, particularly storage areas where sensitive items are kept.

4.4.2.6. Hardware

Security engineering requires the use of burglar-resistant hardware.

The renovation stage provides an excellent opportunity to ensure that good security standards are met. Depending upon the extent of renovation, the opportunity to install surveillance gear is also provided. Some specific areas to consider are:

- Doors with hinges on the secured side, jimmy-and pick-resistant locks and door/doorjamb materials.
- Adequate wiring to support good interior and exterior lighting.
- Burglar- and vandal-resistant glass.
- Buried conduit of adequate capacity to route the cabling of proprietary television and alarm monitoring and control systems.

4.4.3 Summary

Security measures should be considered in any renovation. The best results will be obtained if the security planner has a master plan to guide his efforts. Incorporation of wiring for security alarms, glass partitions for increased surveillance, or upgrading of locks and doors can be accomplished at little increased cost as part of another project although not justifiable by themselves. Security engineering concepts and strategies applicable to facilities construction are equally applicable to renovation.

APPENDIX A

Sources of Consultant Services in Environmental/Industrial Security

This appendix presents a list of firms, companies, and/or individuals who provide consultant services in the area of environmental/industrial security. It is not suggested that all possible sources were exhausted prior to compilation of this list; however, every effort has been made to provide a completely respresentative cross section of expertise.

Because the range of services provided by these firms varies widely -- some are highly specialized (e.g., design and fabrication of devices) and some direct their attention to a broad range of security problems (e.g., human factors, management, hardware) -- this list has been presented alphabetically and coded into four categories that are pertinent to the solution of security problems in industrial or commercial facilities and complexes. Each entry contains the firm's name, address, telephone number, a brief description of the services that firm provides, and category code letters (i.e., P=planning; D=design; C=construction, including hardware design, fabrication and installation; G=general). Many of the firms are coded to more than one category.

Airport Security Council
97-45 Queens Boulevard
Forest Hills, New York 11374

Phone: (212) 275-9300

The Council, which is responsible for developing and administering air cargo loss prevention programs for LaGuardia, Kennedy, and Newark Airports, provides consultants on airport security and security of air cargo. Areas of primary concern are: Personnel security, physical facilities inspection, operational security programs, analysis and evaluation of loss data, and liaison with law enforcement agencies.

(P/D)

Alarm Security Konsultants
Division of Security Architects, Inc.
P.O. Box 182
Medford, New Jersey 90955

Phone: (609) 654-5333

This company provides analysis and assessment of security problems for residential, institutional, educational, industrial, and commercial applications.

The American Institute of Architects
Committee on Architecture for Justice
1735 New York Avenue, NW
Washington, DC 20006

(P)

Phone: (202) 785-7300

This Committee is comprised of architects who are primarily concerned with the planning and design of police and correctional facilities. However, since the members are, by necessity, knowledgeable in the areas of architectural design that impact on criminal justice and crime prevention, they are capable of applying those concepts to virtually any environment. The members of AIA's Committee on Architecture for Justice are as follows:

(P/D)

Raymond C. Abst, AIA
ABST-GROTHE & ASSOC.
624 Scenic Dr.
Modesto, California 95350
209/529-2682

Gerald Deines, AID
Gerald Deines & Assoc. Arch.
136 S. Wolcott
Casper, Wyoming 82601
307/266-2616

Alton L. Akins, AIA
Texas Department of Corrections
Box 99
Huntsville, Texas 77340
713/295-6371

Leroy Andrews, AIA
344 Lynnbrook Avenue
Ventura, California 93003

Joe Boehning, AIA
Boehning, Protz, & Assoc.
2005 Carlisle Boulevard, NE
Alburquerque, New Mexico 87110
505/268-8785

Daniel Boone, Jr. AIA
Boone & Pope, Inc.
224 S. Leggett Drive
Abilene, Texas 79605
915/673-7334

Pamela J. Clayton, AIA
Space for Social Systems
100 S. Patrick St.
Alexandria, Virginia 22314
703/683-1957

Leon Clemmer, AIA
Leon Clemmer & Associates
445 Cedar Street
Jenkintown, Pennsylvania 13046
215/885-6666

Richard G. Conklin, AIA
DMJM
3250 Wilshire Boulevard
Los Angeles, California 90010
213/381-3663

William T. Davis, AIA
12 Washington Park, East
Washington Street
Greenville, South Carolina 29601
803/242-0761

William L. Ensign, FAIA
McLeod, Ferrara & Ensign
5454 Wisconsin Ave. NW
Washington, D.C. 20015
202/652-2775

Sidney J. Folse, Jr., AIA
Folse/HDR
1440 Canal St., Suite 2120
New Orleans, Louisiana 70112
504/525-1444

Robert O. Geary, AIA
Geary, Moore & Aherens, Inc.
1720 Euclid Avenue
Cleveland, Ohio 44115
216/621-7770

Albert Gilbert
Ballinger
841 Chestnut St.
Philadelphia, Pennsylvania 19107
215/629-0900

Thomas E. Greacen, II, FAIA
Greacen, Houston & Rogers
3220 Louisiana, Suite 205
Houston, Texas 77006
713/529-4644

Walter F. Greene, Jr., AIA
Associated Architects
Spring Lane
Farmington, Connecticut 06032
203/677-2801

Robert B. Groenleer
Michigan State Dept. of Corrections
PO Box 30003, Logan Center
Lansing, Michigan 48909
517/373-2461

David B. Hall, AIA
Ellerbe Architects
1 Appletree Square
Bloomington, Minnesota 55420
612/853-2277

Ira Kessler, AIA
The Ofc. of Ira Kessler
980 Benton St.
Woodmere, New York 11598
516/374-1900

George F. Klein, Jr., AIA
Parker, Klein Associates
430 Oak Grove
Minneapolis, Minnesota 55403
613/871-6864

Joseph N. Ladd, AIA
Marcellus Wright Cox & Ladd
1501 N. Hamilton St.
Richmond, Virginia 23230
804/358-7181

Tony R. Lang, AIA
Phillips Swager Assoc., Inc.
3622 Knoxville Avenue
Peoria, Illinois 61603
309/688-9511

Victor D. Langhart, AIA
RNL/Interplan
1610 Arapahoe Street, A-300
Denver, Colorado 80202
303/573-1331

C. Teodore Larson, FAIA
Univ. of Michigan
3575 E. Huron River Drive
Ann Arbor, Michigan 48104
313/971-6274

Patrick Leamy, AIA
HOK
195 Front Street
San Francisco, Calif. 94111
415/271-4848 or 415/986-4275

Jimmy Dan Maddox, AIA
Little-Maddox-Standefer
402 S. Main Street PO 6
Jonesboro, Arkansas 72401

E. Frank McLane, Jr., AIA
100 N. Ashley #800
Tampa, Florida 33602

Robert F. Messmer, AIA
Bureau of Prisons/US Dept. of Justice
320 First Street, NW
Washington, D.C. 20534
202/724-3249

Walter H. Moleski, AIA
Environmental Research Group
1821 Sansom Street
Philadelphia, Pennsylvania 19103

John C. Monroe, Jr., AIA
Monroe & Lefebvre
1021 Pennsylvania
Kansas City, Missouri 64105
816/421-7478

Frederic D. Meyer, AIA
NCCJPA
505 E. Green Street #200
Champaign, Illinois 61820
217/333-0312

Fred G. Owles, Jr., AIA
1819 W. Colonial Drive
Orlando, Florida 32804

Lester C. Pancoast, AIA
Pancoast, Barrelli, Albaisa, Archts.
3370 Mary Street
Miami, Florida 33133
305/442-1193

Caraker D. Paschal, AIA
Finch, Alexander, Barnes, Rothschild & Paschal
44 Broad Street, NW
Atlanta, Georgia 30303
404/688-3313

John McGough, FAIA
Walker, McGough, Foltz, Lyerla
North 120 Wall Street
Spokane, Washington 99201
509/838-8681

Gordon C. Pierce, AIA
219 S. Pennsylvania Avenue
Greensburg, Pennsylvania 15601
412/834-3890

Fred Powers
HOK
100 N. Broadway St.
St. Louis, Missouri 63102
314/421-2000

Ted H. Prindle, AIA
Prindle & Patrick
301 Pierce Street
Clearwater, Florida 33516

Bruce C. Reams, AIA
Orput Associates
1607 North Alpine Road
Rockford, Illinois 61107
815/398-8785

Kenneth Ricci, AIA
The Ehrenkrantz Group, P.C.
19 W. 44th Street
New York, New York 10036
212/889-0099

Harold D. Robertson, AIA
Leo A. Daly Company
8600 Indian Hills Drive
Omaha, Nebraska 68114
402/391-8111

Elliott P. Rothman, AIA
156 Milk Street
Boston, Massachusetts 02109
617/482-5140

Allen L. Patrick, AIA
Prindle & Patrick
199 South Fifth Street
Columbus, Ohio 43215
614/228-3233

Paul Silver, AIA
Gruzen & Partners
1700 Broadway
New York, New York 10019
212/582-7090

Walter H. Sobel, FAIA & Associates
2 North Riverside Plaza
Chicago, Illinois 60606
312/263-6324

George W. Sprinkle, FAIA
Guirey/Srnka/Arnold & Sprinkle
3122 N. Third Avenue
Phoenix, Arizona 85013
602/264-0217

J. Oliver Stein, AIA
Hayes, Seny, Mattern & Mattern
1315 Franklin Road, SW
PO Box 13446
Roanoke, Virginia 24016
703/345-6971

G. John Stevens, AIA
John Stevens Assocs. Inc.
511 East Larned St.
Detroit, Michigan 48226
313/964-0700

Earl S. Swensson, AIA
Earl Swensson Associates
2303 21st Avenue, S., 4th Fl.
Nashville, Tennessee 37212
615/388-2782

William H. Switzer, AIA
Wm. H. Switzer & Assoc.
984 N. Broadway
Yonkers, New York 10701
914/423-5500

Martha L. Rothman, AIA
156 Milk Street
Boston, Massachusetts 02109
617/482-5140

Thomas B. Tucker, AIA
Tucker, Sadler & Associates
2411 Second Avenue
San Diego, California 92101
714/236-1662

Ronald Richard Rucinski, AIA
Donald J. Stephens Assoc. Arch.
41 State Street
Albany, New York 12207
518/462-6551

DeNorval Unthank, Jr. AIA
Unthank Seder & Peticha Architects
259 East Fifth Avenue
Eugene, Oregon 97401
503/342-5777

William H. Vanderbout, AIA
WRDC Architects, Planners, Engineers
150 Ann St. NW
Grand Rapids, Michigan 49502
616/363-9007

Ronald E. Vaughn, AIA
Goat Hill Rd.
PO Box 265
Lambertville, New Jersey 08530
609/397-0801

R. W. Wening, Jr., AIA
Mills, Clagett & Wening
1720 Eye Street N.W.
Washington, DC 20006
202/833-8940

Herbert Wettstein, AIA
N.J. State Div. of Bldg. & Constr.
P.O. Box 1243
Trenton, New Jersey 08625
609/292-5018

W. Gene Williams, AIA
W. Gene Williams & Assocs.
3150 Liberty Tower
Oklahoma City, Oklahoma 73102
405/232-6521

Norman E. Wirkler, AIA
DDKG Architects
1122 Rockdale Road
Dubuque, Iowa 52001
139/583-9131

R. Lamar Youngblood, AIA
Barnes, Landes, Goodman, Youngblood
1000 W. 38th Street, #100
Austin, Texas 78731
512/451-8281

David Miles Ziskind, AIA
Curtis & Davis
126 E. 38th Street
New York, New York 10016
212/689-9590

Anacapa Sciences, Incorporated
P.O. Drawer Q
2034 De La Vina
Santa Barbara, California 93102

Phone: (805) 966-6157

This company provides research, training, and consulting services in the behavioral and engineering sciences. Interest in law enforcement involves: Evaluation of systems, equipment, and procedures from the user viewpoint, evaluation of crime reduction programs, development of law-enforcement techniques and methods, the conduct of pertinent training programs and law enforcement information processing systems. Classes and research emphasize: White-collar crime, urban terrorism, burglary, intelligence analysis, and management and tactical decisionmaking. Services are rendered to government agencies, industries, and commercial concerns.

(G)

Analytical Systems Engineering Corporation
25 Ray Avenue
Burlington, Massachusetts 01803

Phone: (617) 272-7910

This company has experience in law enforcement, criminal justice consulting, and security systems, including the specific areas of sensor applications, human factors considerations, and data base management. The company specializes in objective studies and analyses designed to solve a user's specific problems. For example, systems have been devised to prevent pilferage of inventory data and secrets through the activities of business intelligence and espionage operatives. (G)

Andes Inn Research Center
School of Law, Southern Methodist University
Dallas, Texas 75275

Phone: (214) 692-3380

This organization offers a research capability for police and industrial security forces. Evaluation programs are offered, involving both the selection of a system and the design of evaluation instruments such as rating scales. Implementation and research is combined in the information retrieval systems areas. Associates are experienced in areas such as accounting, law, operations research, and building flow pattern design.

(P/D)

Anticipation, Inc.
410 Jericho Turnpike
Jericho. New York 11753

Phone: (516) 922-8338

This company provides consultation services specializing in internal theft, including the design of closed-circuit television monitoring equipment, pilferage control devices, and cargo security systems.

(C)

Barnes Engineering Company
30 Commerce Road
Stamford, Connecticut 06904

Phone: (203) 348-5381

This company designs and fabricates sophisticated security devices that meet unique government and industrial specifications. Previous customers include the Atomic Energy Commission and the U. S. Army. The firm has government clearances for highly classified work.

(C)

Bellaire Associates
331 Madison Avenue
New York, New York 10017

Phone: (212) 682-2128

This firm, comprised of professional engineers, specializes in management consulting and performs security surveys. In addition, associates conduct security seminars on such topics as the security of high rise buildings.

(G)

Benedict & Myrick, Inc.
Office of Special Services
4332 Rhoda Drive
Baton Rouge, Louisiana 70816

Phone: (504) 293-4260 (Baton Rouge)
(504) 581-4222 (New Orleans)

This company provides security consultation, installs equipment for specific security needs, and custom designs and manufactures security items and systems. Surveillance equipment, closed-circuit television, parking access control, and communications systems are used for deterrence, detection, and control. The company develops security planning for new operations, assists in policy planning and prepares manuals of security procedures and personnel training for "turnkey" programs. Previous experience includes U.S. Army intelligence and security.

(C)

CES Telecommunications
511 Golf Mill
Niles, Illinois 60648

Phone: (312) 297-2366

This company offers architectural and engineering support services for the design of security systems for new buildings or for the remodeling of older structures. Services include the survey of facilities in order to determine security problems.

(P/D)

Don D. Darling & Associates
1100 Glendon Avenue
Westwood Center - Suite 901
Los Angeles, California 90024

Phone: (213) 473-6544

This firm, staffed by scientists, engineers, and security specialists, provides consulting services in such areas as: Planning and analyses of security programs and systems, evaluation and testing of existing systems and programs, security systems support, and evaluation and testing of security systems and equipment. Previous consultation has been provided to a cross section of business, industry, institution, and government/military agencies. The firm's collective problemsolving capabilities have led to the establishment of many security standards.

(P/C)

D-CO-Inc.
P.O. Box 5362
Santa Fe, New Mexico 87501

Phone: (505) 983-1594

This company provides consulting, planning and assessment services for high-level security applications. Capabilities include: Electronic engineering, engineering analysis, planning and layout, cost estimates, and report documentation. Security equipment recommendations are made on the basis of product performance and reliability; essential items can be fabricated when proper off-the-shelf components are not available. Clients have included the U.S. Army and National Guard.

(P/D/C)

Tom Finley & Associates
1511 K Street, N.W., Suite 410
Washington, D.C. 20005

Phone: (202) 293-4327

This firm provides consulting services on the problems of cargo theft and pilferage for industrial and government installations. Services include the development of methods for approaching the problem, hardware recommendations, monitoring of installations, and the training of employees on new security equipment.

(G)

Gage-Babcock & Associates Inc.
9836 W. Roosevelt Road
P.O. Box 270
Westchester, Illinois 60153

Phone: (312) 245-8541

This firm specializes in integrating fire protection, safety, and security into systems design. Criteria for the security of buildings and premises are developed for architects. Problems such as personnel, equipment, and physical structure are examined in risk analyses of present buildings.

(P/D)

Harris & Walsh Management Consultants, Inc.
P.O. Box 698 (271 North Avenue)
New Rochelle, New York 10820

This firm offers comprehensive consulting services on security vulnerability studies, including risk appraisals, dollar loss,

critical loss ratios; countermeasures selection and design, compromising alarms, fences, lights, and other electronic devices; and crime prevention through proper staffing and training of security personnel. Plant protection, fire and disaster control, emergency preparedness, fraud and theft prevention, and the overall protection of physical and informational assets are also areas of capability.

(G)

Richard J. Healy
Building C101, Mail Station 592
The Aerospace Corporation
P.O. Box 92957
Los Angeles, California 90009

Phone: (213) 648-5362

An independent consultant providing services to define the expected hazards to security, and design a defense that applies modern methods and equipment to raise the security level and reduce protection costs. All aspects of potential designs are covered, from plant layout to locks to alarms and lighting.

(G)

Lewis H. Irving, Consultant
Department of Sociology
Central State University
Edmond, Oklahoma 73034

Phone: (405) 341-2980 x2533

An independent consultant who provides social survey research to government agencies and businesses, specializing in defining the human factors approach, both in defining the environment necessary to produce social change and social integration, and in identifying types and kinds of equipment needed to work on the problem.

(P)

Management Safeguards, Inc.
National Headquarters, Two Park Avenue
New York, New York 10016

Phone: (212) 532-7150

The Consulting Division of Management Safeguards offers surveys of physical security, operational procedures, and accounting controls to identify exposures to loss, and to enable development and implementation of security plans. Physical security planning defines the need for alarm and locking devices, employee and visitor controls, communications, lighting, access controls, shipping and receiving dock protection, annunciator consoles, manpower deployment, and security requirements in new buildings or existing facilities.

(G)

Marlborough Intelligence
P. O. Box 13
Upper Marlboro, Maryland 20870

Phone: (301) 952-0909

This firm offers a variety of services, including security consulting. Procedures consist of investigation of activities such as internal theft, embezzlement, and pilferage; consulting services are available for the design of internal controls for personnel, equipment, and premises. Recommendations for security systems are made for business and industry after surveys of premises and operations.

(G)

McManis Associates, Inc.
1120 Connecticut Avenue, N.W.
Washington, D. C. 20036

Phone: (202) 296-1355

This firm employs systems engineering methodology to develop pre-architectural specifications for operational configurations including security. Attention is given to security program planning and evaluation, defining objectives, identifying protective needs, and allocating resources.

(P)

George P. Morse & Associates
Consultants in Protection
9402 Stateside Court
Silver Spring, Maryland 20903

Phone: (301) 434-3245

This firm performs, studies, provides training, and recommends operational and physical improvements in the area of crime and loss prevention. Specializing in institutional security, particularly hospitals, they perform objective studies and recommend specific solutions. Security systems design and installation support can also be provided.

(P/D)

Mt. San Antonio College
Department of Public Safety and Service
110 North Grand Avenue
Walnut, California 91789

Phone: (213) 339-7331
(714) 595-211 x252, x324

This organization provides staff personnel who analyze and interpret research data, which are then applied to the design and development of security-related programs.

(P/D)

Robert James Obenland
P. O. Box 139
Concord, New Hampshire 03301

Phone: (603) 284-6407

An independent consultant who provides services in research, programming, architectural design, and postoccupancy evaluation for the built environment. Previous experience has included areas such as architectural and environmental security analyses for courts and correctional facilities, and design assistance focusing on crime prevention and humanization in public housing.

(P/D)

James W. O'Neil, Inc.
25 Massachusetts Avenue
Braintree, Massachusetts 02184

Phone: (617) 843-8653

An independent consultant specializing in preventing losses from burglary, employee theft, robbery, vandalism, espionage, and other criminal activities. Consultation is available for help with problem assessment, analysis of procedures and techniques, improvement in security equipment and service, supervision of acquisition and installation of systems and devices and review of overall security conditions. Surveys include the evaluation of physical security arrangements, review of personnel hiring and training in security, comparison of security policies versus actual practices, and recommendations for developing and implementing security programs.

(G)

PRC Public Management Services, Inc. (PRC/PMS)
7600 Old Springhouse Road
McLean, Virginia 22101

Phone: (703) 893-1830

This company provides services to public and private agencies for organizational and management analysis, program evaluation, resource allocation, information systems design and implementation, facilities design, crime-specific planning, evaluation of anticrime countermeasures, design of correctional systems, and the training of personnel for administration, fiscal control and reporting.

(P/D)

Pacemaker Planning
3617 Lexington Road
Louisville, Kentucky 40207

Phone: (502) 897-5756
(502) 454-0225

This firm analyzes, evaluates, and makes recommendations on how to reduce the loss of cash and high-value merchandise due to employee theft, shoplifting, armed robbery, and burglary. Crime reduction recommendations emphasize environmental redesign through attention to lighting arrangements, display techniques, interior design, exterior landscaping and control of parking patterns, aisle and customer-flow control, and management and employee training. Recommendations focus on changes in business procedures and physical plant modifications, rather than on installation of hardware devices or use of sentry personnel.

(P/D)

John W. Powell Consultants, Inc.
2600 Dixwell Avenue
Hamden, Connecticut 06514

Phone: (203) 248-2985

This firm specializes in the security problems of large, complex installations such as college and school campuses, utility and insurance companies, atomic power stations, business and industrial establishments, and computer centers. Assistance is also provided to architects in the planning and design of security systems and

programs for new facilities such as civic centers, large shopping/ office complexes, high-rise apartments, and condominiums. All services include analysis, study, recommendations for equipment and procedures, bid specifications, and training as required.

(G)

Profitect Inc.
Professional Protection Consultants
At Wharfside, 680 Beach Street
San Francisco, California 94109

Phone: (415) 283-3802
(415) 283-0511

(213) 786-4605 Los Angeles

This firm provides consultation for comprehensive protection programs, as well as systems and engineering guidance in equipment selection to architects, commerce, industry, hospitals, financial institutions, and data centers.

(C)

Protection Systems
10961 Bloomfield Street
Los Alamitos, California 90720

Phone: (213) 430-0786
(714) 826-0880

This firm offers security consultation and design work for public utilities, major shopping centers, large professional buildings, government agencies, state prisons, and police agencies, with some custom design of equipment. Specialties include: Design layout, installation, and maintenance of outdoor systems and access control, central alarms, and closed-circuit television.

(G)

Warner Consultants
75-A G Street, S. W.
Washington, D. C. 20024

Phone: (202) 737-0255

This company engages in research and development of security systems, which includes site evaluation system design and development.

The firm has carried out studies of this kind for industrial and commercial organizations, associations, and government agencies, emphasizing the effect of building design and location on security. Work has included developing a residential security planning and design guide and drafting a compendium of building concepts.

(C)

Westinghouse National Issues Center (WNIC)
2341 Jefferson Davis Highway
Suite 1111
Arlington, Virginia 22202

Phone: (202) 833-5959

The Westinghouse National Issues Center conducts studies on factors influencing criminal activity for governmental agencies; designs, assists in the implementation of, and evaluates demonstrations implementing crime prevention strategies; and provides consulting services to cities and authorities on crime prevention strategies in facilities design and operations. Demonstrations have been designed and implemented in such environments as schools, commercial/industrial, and residential. Typically, consulting on Crime Prevention Through Environmental Design (CPTED) techniques has been provided to a committee responsible for security design of a transportation/commercial/hotel complex, and to an authority responsible for redevelopment of an industrial area.

(G)

APPENDIX B

Annotated Bibliography

This appendix is a selected bibliography of source materials that address environmental and industrial security, particularly as they relate to the planning, design, and construction of new facilities and industrial complexes.

The entries are presented alphabetically by corporate author and are indexed by subject, title, and individual author.

1. Alexander, Alfred, and Val Moolman. Stealing. New York, NY: Cornerstone Library Publications, 1969.

This is a guidebook for management personnel on how to reduce their losses by bringing the incidence of pilferage under control. This book exposes the tricks of thieves and provides management with tips on how to beat the game.

2. Berla, N. The Impact of Street Lighting on Crime and Traffic Accidents, Library of Congress Legislative Reference Service, Washington, D. C. 1965.

The article surveys the findings of studies performed in various U.S. cities and concludes that fewer crimes and street accidents followed a significant increase in the level of street illumination.

3. Blanchard, Janelle. "Proposal for a Model Residential Building Security Code," p. 1-25. In U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Deterrence of Crime In and Around Residences.

Deals with the physical design elements that might be incorporated into building codes as a means of residential crime prevention. Emphasizes the need for uniform building codes to improve industrialized housing, but states that security codes must recognize differing needs.

4. Brill, W. H. "Security in Public Housing: A Synergistic Approach," p. 26-43. In U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Deterrence of Crime In and Around Residences.

Looks toward a mix of project security improvements, including target hardening approaches and measures to increase the social cohesion of the residents, which together would produce a synergistic effect. Mentions the Innovative Modernization Project (IMP), in which were tested and evaluated ways to improve the quality of life in public housing.

5. California. Council on Criminal Justice. Selected Crime Prevention Programs in California. Sacramento, CA: Council on Criminal Justice, 1973.

Reports on crime prevention programs in use in California that focus on action that can be taken before crimes occur, based

on questionnaires and a series of onsite visits to 172 law enforcement departments. Included are the program's purpose, past results, recommended implementing procedure, possible problem areas, costs, and recommended forms and literature. Reviews programs dealing with areas such as crime prevention units, facility planning, property identification, residential, commercial, and industrial security inspections, and commercial robbery prevention.

6. _____. Department of Justice. "On the Alert! How to Protect Your Business and Property," California Department of Justice Information Pamphlet No. 4, prepared by Evelle J. Younger, Attorney General, August 1973.

This pamphlet briefly discusses how businessmen can guard against shoplifting, employee theft, bad checks, robbery, and burglary in new and existing facilities. Site selection, building placement, parking, perimeter controls, lighting, and traffic flow all are cited as important considerations.

7. _____. Department of Justice. Attorney General's Building Security Commission. Building Security Standards -- Preliminary Report to the California Legislature. Sacramento, CA: Department of Justice, January 1973.

Defines the problem of creating and maintaining physical security and establishes a logical approach for developing building security standards. Concentrates on the physical aspects of elements in barrier systems, with emphasis on window and door elements as being the most frequently attacked.

8. _____. University. Space Sciences Laboratory and Center for Planning and Development Research. Discouraging Crime Through City Planning, by Shlomo Angel. Prepared for the National Aeronautics and Space Administration. Working Paper No. 75. Berkeley, CA: University of California, February 1968.

The author proposes that environmental prevention can forestall crime, and focuses on the characteristics of areas where crime occurs. He hypothesizes that crime is a function of opportunism, and that areas of high-crime density are typically easily accessible to and well known by the criminal, are known to offer high likelihood of finding a victim at a given time, and involve little risk of police apprehension. With emphasis on intensity of use as a major factor in crime occurrence and the hypothesis of a critical use intensity zone, the author suggests

adjustment of intensities of pedestrian circulation channels as an environmental design solution. By means of 13 alternative design configurations, he indicates how specialized activity areas like industrial areas can be evaluated at night, evening establishments centralized, and strip commercial developments altered to either decrease or increase intensity of use so as to avoid the critical high-crime intensity zone.

9. Cedar Rapids, Iowa. Police Department. Installation, Test, and Evaluation of a Large-Scale Burglar Alarm System for a Municipal Police Department -- Second Phase Completion Report. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. Cedar Rapids, IA: Cedar Rapids Police Department, December 1971.

   Describes the effectiveness of a simple and inexpensive central station burglar alarm system installed under police supervision in 350 businesses in Cedar Rapids. Interim results from the program indicate that the alarms are effective in improving police arrest and clearance figures, but not necessarily effective in deterring burglars.

10. Center for Residential Security Design. Design Directives for Achieving Defensible Space, by Oscar Newman. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. New York, NY: Center for Residential Security Design, June 1973.

    This is a handbook for housing officials, architects, and urban planners. Gives instructions for providing residential security through employment of hardware and security personnel, and is directed toward the initial design and programming of new residential developments. Discusses building codes and the problems the present code structure creates in providing security.

11. Cherico, P. "Security Requirements and Standards for Nuclear Power Plants," Security Management, 18(6): 22-24, January 1975.

    Reviews present and proposed security requirements to protect against acts of sabotage and against the diversion and misuse of special nuclear materials. The present requirements of the Atomic Energy Commission and the American National Standards Institute are examined. Among the areas covered in these standards are the use of a physical security plan, security guards, alarm systems, and general security systems.

Projected requirements in the areas of materials and plant protection, personnel selection, training, and access control also are discussed.

12. Colling, Russell L. Hospital Security: Complete Protection for Health Care Facilities. Culver City, CA: Security World Publishing Co., Inc., 1976.

    This book examines the entire field of health care protection, developing a detailed, practical program for establishing a security system or refining existing programs. Hospital vulnerabilities and the security function are analyzed in depth, including security administration and operations, preventive programming, emergency operations, and special problems. Such diverse areas as hiring and training, records and reports, psychological deterrents, disaster planning, and drugs and pharmacy controls are covered. The information presented is intended to bring to top level management a basic understanding of protection needs, provide the security administrator with operational guidelines and practical program suggestions, and give the line officer and supervisor a background which will enable them to better understand health care security systems and their interaction within the operational program. A subject index is included.

13. Cooper, Clare. "St. Francis Square: Attitudes of its Residents," AIA Journal, 56(6): 22-27, December 1971.

    Treats the effect of environmental design on attitudes of residents of a city housing project, and provides an example of the apparently successful incorporation of "territorial" design principles in housing projects.

14. "Cost of Crimes Against Business," Security Management, 19(1): 6-14, March 1975.

    Summary of the available knowledge of industry and the Federal government on the extent of the dollar loss of American business to crime in the period since 1971. Discussed individually are: Bad checks, counterfeiting, inventory shortages, robbery, vandalism, and other crime-related problems. Crime prevention measures are outlined.

15. Dillingham Corporation. SUA Division. A Study of Crime Prevention Through Physical Planning. Prepared for Southern California Association of Governments. Los Angeles, CA: Dillingham Corporation, September 17, 1971.

Provides information on existing or proposed techniques for achieving security in future residential, commercial, industrial, institutional, and recreational developments through the manipulation of the physical characteristics of these developments. Focuses on the planning of future developments, and urges that similar efforts be directed toward modification of existing structures.

16. Educational Facilities Laboratories, Inc. Designing Schools to Minimize Damage from Vandalism and Normal Rough Play. Schoolhouse Newsletter No. 15. New York, NY: Educational Facilities Laboratories, Inc., 1974.

Based upon a study conducted by Professor John Zeisel, Graduate School of Design, Harvard University. Briefly describes four categories of vandalism and suggests possible design responses to minimize the burden of cost resulting from vandalistic activities.

17. Educational Resources Information Center. ERIC Clearinghouse on Educational Management. School Security, by Nan Coppock. Educational Management Review Series No. 23. Eugene, OR: University of Oregon, October 1973.

Explores briefly the general dimension of crime in public schools, inventories the types of antivandalism techniques in current use, and cites data on the incidence of crimes against persons occurring in schools.

18. Fireman's Fund Insurance Company. Protecting Your Business from Embezzlement, Burglary, and Robbery. San Francisco, CA: Fireman's Fund Insurance Company (P.O. Box 3395, San Francisco, CA 94119).

This booklet outlines conditions or actions that facilitate crimes against businesses and offers several countermeasures. Discussed are problems of internal security; control of vulnerable areas such as receivables, purchases, and inventories; physical security; and mechanical crime prevention methods.

19. Fortune, Thomas. "Schools Equipped with 'Ears' to Fight Vandalism," Los Angeles Times, September 5, 1973.

Describes a sound monitoring intrusion alarm system being installed in the Placentin, Orange, and Santa Ana unified

school districts to prevent vandalism and burglary. The commercially available system utilizes a public address speaker that is set to trip a light at police headquarters when noise exceeds a predetermined level, allowing the dispatcher to listen in on whatever triggered the alarm.

20. Gocke, B. W. Practical Plant Protection and Policing for the Security of Business and Industry. Springfield, IL: Charles C. Thomas, 1957.

Studies the requirements for effective, efficient business and industrial security protection and recommends methods of application. Provides a working basis for increased profits by virtually all types of enterprises by analyzing factors involved in the physical security of facilities (e.g., access control).

21. Griffin, R. K. "Theft Against Retail Profit: A Management Perspective," Security World, 9(4): 14-15, 17-20, April 1972.

Guidelines for evaluating the cost of shoplifting, curbing employee theft, and involving employees in theft prevention programs.

22. GTE Sylvania Incorporated. Security Systems Department. An Evaluation of Small Business and Residential Alarm Systems, by T. P. Chleboun and K. M. Duvall. 2 v. Prepared for U. S. Department of Justice, Law Enforcement Assistance Administration. M-1442. Mountain View, CA: GTE Sylvania Incorporated, June 1972.

Presents a comprehensive discussion of the role of various alarm systems, including information about offenders and an analysis of the crime risk characteristics of various categories of alarm users. Evaluates alarm systems in terms of "threat probability," and presents a shopping list of applicable equipment. Provides offender and victim profiles, correlated with variations on a particular crime deterrent (alarm system).

23. Healy, R. J. Design for Security. New York, NY: Wiley, 1968.

Analyzes the optimum security layout for industrial facilities, starting with the premise that security can, at best, provide only physical controls that act as "impediments to the undetermined." In the context of this book, security is intended not only as protection against common-law crimes such as theft but also against industrial espionage and sabotage.

24. Hemphill, C. G., Jr. Security for Business and Industry. Homewood, IL: Dow Jones-Irwin, 1971.

Methods for reducing business losses due to theft, vandalism, fire, burglary, embezzlement, and other problems. Discusses physical aspects of business security from the selection of plant location and actual building of the plant to an assortment of alarm devices and protective services. Sound procedural controls are detailed, which apply to purchasing and receiving, warehousing and stockkeeping, shipping and deliveries, control of merchandise in sales areas, and the handling of cash receipts.

25. Holcomb, R. L. Protection Against Burglary. Iowa City, IA: State University of Iowa Institute of Public Affairs, 1973.

Describes to potential victims the things they can do to thwart burglars and to reduce their losses in the event of burglary. Concludes with surveys for use in commercial buildings and residences.

26. Hughes, M. M. (ed). Successful Retail Security: An Anthology. Los Angeles, CA: Security World Publishing, 1973.

Presents articles (reprinted from the professional security magazine, Security World) on methods and programs that retailers have used to counter a broad range of crimes and other hazards.

27. Jacobs, Jane. The Death and Life of Great American Cities. New York, NY: Vintage Books, 1961.

Attacks the current city planning procedures of functional separation of types of land use. Maintains that, in designing new urban environments, planners ignore the most basic structure of the city -- the intricate and closely connected diversity of uses that constantly reinforce one another economically and socially.

28. Kentucky. University. College of Engineering. Office of Research and Engineering Services. Proceedings of the 1973 Carnahan Conference on Electronic Crime Countermeasures, Lexington, Kentucky, May 1-3, 1972. Compiled by J. S. Jackson and R. W. DeVore. Prepared in cooperation with the Institute of Electrical and Electronics Engineers. Lexington, KY: University of Kentucky, 1973.

Presents a compendium of papers on the design and application of various electronic surveillance, alarm, and information processing systems.

29. Kingsbury, A. A. Introduction to Security and Crime Prevention Surveys. Springfield, IL: Charles C. Thomas, 1973.

    Provides a reference text for police officers, professional security consultants, and college-level students of security. Offers step-by-step guidelines for conducting onsite examination and analysis of premises to identify physical opportunities for crime and to develop methods for reducing such opportunities.

30. Knight, P. E., and A. M. Richardson. The Scope and Limitation of Industrial Security. Springfield, IL: Charles C. Thomas, 1963.

    The authors examine the reasons for and purpose of industrial security, defining its nature and limitations both in general and in reference to various professional methods, operations, and mechanics.

31. Kwan, Q. Y. Scope, Nature, and Prevention of Vandalism. Prepared for the U. S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, 1972.

    Short- and long-range approaches to the problem of vandalism are proposed. Architectural and environmental design considerations figure prominently in short-range proposals. Some suggestions are unbreakable glass, fenceless parks, well-lighted public areas, and concrete-encased plumbing fixtures.

32. Liechenstein, Michael. Designing for Security. Paper presented at the American Institute of Aeronautics and Astronautics Urban Technology Conference, New York, N.Y., May 24-26, 1971. P-4633. New York, NY: The Rand Corporation, (n.d.).

    Suggests the need for cooperation among architects, security experts, social psychologists, and government agencies during the planning phases of new buildings. Critical to crime prevention is the demarcation, arrangement, and hierarchy of public and private areas at the

building conception. The high post-construction costs of implementing security measures are stressed, as is the benefit of multifunctional integrated design units providing fire, burglary, robbery, and utility protection.

33. Loss Prevention Diagnostics, Inc. Three Solutions in Reduction of Criminal Opportunity in Mass Transportation. A Selection of Devices and Techniques to be Demonstrated in Mass Transportation. Prepared for City of Chicago, Department of Public Works, Transit Security Study. Caldwell, NJ: Loss Prevention Diagnostics, Inc., June 15, 1973.

    Presents in detail three solutions developed for Chicago Transit Security Project. Gives potential implementation sites, hardware requirements and possible suppliers, and estimated costs for each of these solutions. Also describes modified construction and lighting to enhance surveillance.

34. Luedtke (Gerald) and Associates. Crime and the Physical City, by Gerald Luedtke et al. Prepared for U. S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. Detroit, MI: Gerald Luedtke and Associates, 1970.

    Analyzes the importance of selected physical features to the crime of robbery and burglary, including the conditions and maintenance of buildings, streets and alleys, lighting, mixtures of land use, rates of pedestrian flow, landscaping, visibility of entrance and exit points. The data base used is an inventory of physical features in 289 structures in which crimes have been recorded by the Detroit Police Department.

35. Malt (Harold Lewis) Associates, Inc. Tactical Analysis of Street Crimes, by H. L. Malt et al. Prepared for City of Jacksonville, Fla., Office of the Sheriff. Washington, DC: Harold Lewis Malt Associates, Inc., 1973.

    Examines the relationship between the physical street environment and street crime, specifically whether certain environmental indicators (e.g., bushes, abandoned buildings) affect the location and incidence of street crime; whether users, offenders, and policemen are aware of this effect; and whether their behavior is influenced by their perception of the environmental indicators.

CONTINUED

1 OF 2

36. Mandlebaum, A. J. Fundamentals of Protective Systems: Planning/Evaluation/Selection. Springfield, IL: Charles C. Thomas, 1973.

Provides a basic survey and comparative evaluation of the protective systems currently available for both business establishments and private systems. Emphasizes security devices as opposed to design factors.

37. Maurer, E. C. "Housing Project Safety Restored," Journal of Housing, 28(6): 282, June 1971.

Indicates that lighting proved effective in one housing project in reducing vandalism, muggings, and other crimes.

38. Michigan. University. Impact of Street Lighting on Street Crime, by Roger Wright, et al. 2 v. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. Ann Arbor, MI: University of Michigan, May 1974.

Describes an investigation of the crime deterrent effects of upgrading street lighting from incandescent to mercury and sodium vapor in selected high-crime commercial and residential areas in Kansas City, Missouri. The two areas are commercial, located in the central core, and residential, in an adjacent zone. Effectiveness is asserted by comparing changes in crime rates before and after installation in both relit and nonrelit areas. Crimes of violence are significantly deterred, while crimes against property are largely unaffected.

39. Moolman, V. Practical Ways to Prevent Burglary and Illegal Entry. New York, NY: Cornerstone Library, 1970.

Various modi operandi of burglars, with concise and practical descriptions of security hardware and measures for burglary protection and prevention. Aspects of security ranging from architectural design to effective use of lighting are discussed. The designs and operations of locking devices are described along with recommendations for their proper use. The different types of alarm systems are explained. Theft prevention measures covered include applications to residential, commercial, and automobile security.

40. Morse, G. P. Protecting the Health Care Facility: A System of Loss Prevention Management Effective for All Industry. Baltimore, MD: Williams and Wilkins Company, 1974.

The responsibility for security and protection of property and persons is considered to be that of the management. The procedure for developing and implementing a protection plan is presented. Accident prevention, fire prevention, radiation safety, asset protection, and personnel protection are discussed. Access control, data processing, key control and masterkeying, parking administration, and construction review are identified as important procedures for reducing loss and accidents.

41. Murphy, H. J. "Security of Airport Parking Lots," Security Management, 19(2): 22-25, May 1975.

This article discusses the physical security of airport parking lots in particular, based on principles that have been used and proved effective in industrial, educational, and health facilities. Emphasis is on designing security into the lot to eliminate targets of opportunity and prevent or deter criminal activity. This is achieved through a combination of design techniques and human cooperation.

42. Murphy, Ralph. "Design for Physical Security," Security Management, 20(20): 12, 14, March 1976.

In this article, the author emphasizes that "the most effective way... in establishing operational security requirements is in the new construction stage, 'before' the design is accepted and becomes firm." Based on this, general architectural/security considerations are discussed (e.g., access control, traffic flow) as well as some specific strategies to achieve desired results.

43. Murphy, Ralph, and William Norman. "Physical Security: Chance, Choice, Change," Security Management, 20(2): 8-10, March 1976.

This article defines physical security and discusses applications through deterrent, interior, and internal protection. For example, the authors cite that criminal activity can be deterred through "Proper design or configuration changes in a facility's perimeter, lighting changes..."

44. "Need for Security in Buildings More Demanding," Engineering News Record, 189(11): 25-33, September 14, 1972.

Discusses hardware countermeasures to crimes in office and residential buildings.

45. New Mexico. University. Institute for Social Research and Development. Transfer Potential of Crime-Specific Programs to Metropolitan Albuquerque, by G. S. Metarelis. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration. Albuquerque, NM: University of New Mexico, November 1972.

Discusses recent techniques used to counter crime, and describes crime prevention programs in seven large cities with respect to methods and results. Includes model building-security ordinances for Seattle and Oakland.

46. New York, New York. Street and Highway Safety Lighting Bureau. Out of the Shadows. New York, NY: New York, (n.d.)

Shows how street lighting can help reduce crime and traffic accidents.

47. New York City Rand Institute. Improving Public Safety in Urban Apartment Dwellings: Security Concepts and Experimental Design for New York City Housing Authority Buildings, by William Fairley and Michael Liechenstein. R-655-NYC. New York, NY: The Rand Corporation, June 1971.

Addresses the reduction of crime in the New York City Housing Authority's existing public housing facilities. The three crimes of particular interest are vandalism, robbery, and burglary. The purposes of this project are to define the problem and security alternatives, develop guidelines for estimating the cost effectiveness of security alternatives, and develop experimental models to evaluate the estimated effectiveness of different security measures.

48. Newman, Oscar. "Architectural Design for Crime Prevention," p.52. In U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Deterrence of Crime In and Around Residences.

Describes defensible space as a form of crime prevention that, while basically mechanical, also acted as a form of corrective prevention, alleviating some of the causes of criminal behavior.

49. _____. Defensible Space: Crime Prevention Through Urban Design. New York, NY: Macmillan, 1972.

Develops the concept of residential security predicated on a positive correlation between architectural design and behavior. While the author does not claim that design can mandate behavior, he posits that the forms of an environment can elicit responses from the inhabitant of that environment that can enhance his security. On the simplest level, architects can create or prevent encounters. Latent attitudes of territoriality, the acknowledgment that a space is a domain that warrants protection, and the increased awareness of "spheres of influence" on the part of the young will operate to inhibit crime both "mechanically" and "correctively." This territoriality, fostered by physical means -- grouping dwellings in a residential complex, defining and differentiating grounds, providing means for natural surveillance, positioning routes -- is essential to a self-defending community. Crime is deterred when the easy opportunity to vandalize, rob, burglarize, or rape is thwarted by the territorial prerogative of residents.

50. Panhandle Regional Planning Commission. A Study of Building Codes as Related to Crime Prevention, by Peat, Marwick, Mitchell and Company. Prepared for U.S. Department of Housing and Urban Development, and for Texas Criminal Justice Council. Amarillo, TX: Panhandle Regional Planning Commission, September 1972.

This document is the report of a HUD/Texas Criminal Justice Council pilot study to determine the relationship between building codes and crime prevention. Part I presents a general survey of trends of burglary and related offenses nationwide and in the Panhandle area. In Part II, the findings to date of research programs in the field are summarized.

51. Post, R. S., and A. A. Kingsbury. Security Administration -- An Introduction. Springfield, IL: Charles C. Thomas, 1973.

Presents an introductory text on the background, components, and programming of government and proprietary security activity for security and law enforcement personnel.

52. Salama, Ovadia, and Alexandria Tzonis. "Strategies for Defense," Progressive Architecture, (4): 72-72, April 1974.

Describes the development of a framework for generating crime-reducing features in a variety of environments and transferring Newman's findings from the area of public housing to other environments.

53. San Luis, Edward. Office and Office Building Security. Los Angeles, CA: Security World Publishing, 1973.

Discusses those areas most likely to be identified as criminal activity (i.e., burglary, robbery, arson, violence, and industrial espionage). Evaluates security techniques that have proven most successful in identifying and defending against problem areas quickly and efficiently.

54. Sears, H. Crime, Vandalism, and Design. Paper presented at the Crime Prevention Workshop held at the University of Toronto, Centre of Criminology, May 20-22, 1975. Toronto, Ontario, Canada: University of Toronto, Centre of Criminology, 1975.

Examines background information on the relationship of crime and environmental design, and explores the means by which physical environments can be designed and modified to reduce vandalism and crime. It is noted that such building features as impersonal spaces, lack of needed facilities, overcrowding, and unsurveillable spaces promote crime and vandalism.

55. Sommer, Robert. Personal Space: The Behavioral Basis of Design. Englewood Cliffs, NJ: Prentice-Hall, 1969.

Discusses the psychology of designing space. The basic premise is that spatial relationships affect user behavior in a quantifiable fashion and in other more complex and less measurable ways. The treatment is philosophical and speculative; however, specific studies of the effect of spatial arrangements on social interaction are described.

56. Southern California Association of Governments. Handbook of Crime Prevention Bulletins: Crime Prevention Through Physical Planning. Los Angeles, CA: Southern California Association of Governments, 1971.

Draft of 16 single-topic bulletins that provide information on how to prevent crime through the planning and design of physical characteristics and their application to specific projects, such as apartment complexes, industrial parks, commercial recreation developments, and public buildings.

57. Thornsen, J. E. "Air Cargo Security: A Concept that Works," Security World, 10(6): 28-31, 34-35, June 1973.

This article discusses the security problems of an air freight company and procedures, electronic devices, and systems used to reduce loss at Kennedy Airport in New York, and describes the security measures undertaken to reduce overall losses from freight damage and theft. Reports on the security actions taken to reduce opportunity for snatch-and-run thievery, forgery, or pilferage. Procedures described include the architectural redesign of space to enable cargo containment and clear observation, the installation of closed circuit television at key points, the systematic recording and tracing of cargo throughout the process, the required use of a special stamp to guarantee pickup authority, and the tightened processing of truckers making pickups. The handling of sensitive merchandise using a special security cage is also described. Dramatic reduction in loss was reported.

58. Tyska, L. A. "Security Lighting for the Cargo Terminal," Security Management, 20(3): 40-41, July 1976.

This article, which is based on the premise that use of lighting is an effective deterrent to criminal activity, discusses what proper and adequate lighting is. Discussed are recommended light levels and location points.

59. U. S. Congress. Senate. Crime Against Small Business. A Report of the Small Business Administration Transmitted to the Select Committee on Small Business. S. Rept. 91-14, 91st Congress, 1st Session, 1969.

Provides a benchmark of current problems and solutions to crime, so as to encourage optimum use of existing crime prevention measures (particularly, protective devices, architectural design, and managerial systems) and to encourage the provision of more effective crime insurance. The main orientation of the study is specifically the small businessman and real-world remedies on a cost/benefits basis.

60. U. S. Department of Housing and Urban Development. Office of Policy Development and Research. Division of Building Technology. A Design Guide for Improving Residential Security, by Oscar Newman; Center for Residential Security. HUD Guideline 2. Washington, DC: Government Printing Office, December 1973.

Presents the thesis that a well-designed residential security system is one with a functioning interrelationship between the various component parts. Each element is examined in separate chapters. This text directs its attention primarily to the creation of fortifications because, "it is the easiest to implement after the act of building is completed, whereas defensible space concepts are best achieved in a project's inception."

61. U. S. Department of Justice. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Architectural Design for Crime Prevention, by Oscar Newman; New York University, Institute of Planning and Housing. Washington, DC: Government Printing Office, March 1973.

Updates the observations on environmental design originally presented in Newman's Defensible Space (q.v.). Discusses the concept of "defensible space" and human territorial instincts, and reviews the works of other authors, as they relate to defensible space. Relies heavily on pictorial rather than tabular presentation.

62. _____. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Minimum Building Security Guidelines and Cost Estimate for the Security Features. Initial Draft. Prepared in Cooperation with the Federal Insurance Administration, Department of Housing and Urban Development. Washington, DC: Department of Justice, May 14, 1971.

Contains a model security code covering minimum standards for doors, windows, safes, and alarms for commercial and residential buildings. Standards are expressed largely in design rather than performance factors.

63. _____. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Urban Design, Security and Crime. Proceedings of a Seminar in Washington, D. C., April 12-13, 1972. Compiled by R. M. Rau. Washington, DC: Department of Justice, January 1973.

Focuses on security measures for preventing burglary and stranger-to-stranger crimes in and around residences and businesses in the urban community. Reviews the state-of-the-art, and develops proposed research and action ideas for the future.

64. _____. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Law Enforcement Standards Program. Directory of Security Consultants, by Elizabeth Robertson and John V. Fechter; Center for Consumer Products Technology, National Bureau of Standards, Washington, DC: Government Printing Office, October 1975.

This is a directory of security consultants available to assist the consumer in solving security problems. The resources listed in this document should be of help to the general public, community authorities, police, businesses, and others wishing to identify known and effective strategies to eliminate or protect targets of opportunity, in addition to identifying measures and mechanisms to stimulate community support of such strategies. While the scope of this directory is limited primarily to targets of opportunity, the protection of high security targets is within the competence of some of the individual resources that are listed.

65. U.S. Department of the Army. Physical Security. FM 19-30. Washington, DC: Department of the Army Headquarters, February 17, 1965.

Presents material that is applicable to the security problems of both military and industrial installations. Includes a physical security checklist.

66. U. S. Department of Transportation, Office of the Secretary. Guidelines for the Physical Security of Cargo. Washington, DC, May 1972.

Presents guidelines to assist transportation management in stemming the over-$1-billion annual loss due to cargo theft and pilferage. Because analysis of these problems revealed that 85 percent of cargo stolen is removed by authorized persons or vehicles, the guidelines are directed towards methods against internal threats.

67. Ursic, H. S., and L. E. Pagano. Security Management Systems. Springfield, IL: Charles C. Thomas, 1974.

Establishes a systems approach to organizational security management. Emphasis is on a total (viewing the organizational entity as a whole) and open (to society) systems approach to the management functions related to the organizational function of security. Organizational security is

defined as a service function whose purpose is to develop a social awareness for the protection of life and property within private and public institutions as a collective responsibility complementing law enforcement.

68. Walsh, T. J., and R. J. Healy. Protection of Assets Manual. Santa Monica, CA: The Merritt Company, 1975.

This manual, which is supplemented monthly, is a two-volume source document for obtaining data on any protection problem. Information contained in the manual covers the broad range of subject areas required to protect the modern enterprise from nonbusiness losses.

69. Ward, C. Vandalism. London, England: Architectural Press, 1973.

A collection of articles examining vandalism, with emphasis on related psychological, sociological, economic, and architectural considerations, drawing upon British and American experience. Initially, an attempt is made to go beyond the concept of vandalism as meaningless violence. Vandalism is shown to have both expressive and instrumental value. It can be a form of social protest, a reaction to environmental stimuli, or even an attempt to assert one's masculinity. Professional responsibilities of the architectural designer are examined. The authors show how design considerations can minimize the impetus and opportunities for vandalism, as well as its consequences. Legitimized vandalism is seen in the examples set by motorists, industry, government, and others who noncriminally damage the environment. Finally, solutions are proposed, such as deflection of the behavior to other less harmful, or constructive, alternatives. Legislation, community action, and education, improved protection and detection methods, and punitive deterrence methods also are explored.

70. Weber, T. L. Alarm Systems and Theft Prevention -- An Expert Says: "Think Like a Thief." Los Angeles, CA: Security World Publishing, 1973.

Discusses top-security alarm systems, the methods by which they are being defeated, and the countermeasures currently available against such methods. Explains the economics of alarm system choice, as well as the problems of police-connected alarms, the types of safes that can prevent successful attacks, and the pros and cons of the proprietary alarm located on the premises.

71. Wright, K. G. Cost-Effective Security. New York, NY: McGraw Hill, 1973.

Presents a general introduction to securing all types and sizes of business against internal pilferage and crimes against property perpetrated by outsiders. Addressed to business managers, it discusses in layman's terms many issues pertaining to security.

72. Westinghouse Electric Corporation. Justice Institute. Cargo Security Survey of the Port of Hampton Roads. Prepared for the U. S. Department of Justice, Law Enforcement Assistance Administration. Arlington, VA: Westinghouse Electric Corporation, November 1973.

Presents the findings and recommendations of a cargo security survey of five waterfront installations for improved security as may be realistically implemented with minimum increased cost. Among others, the recommendations provided cover: Perimeter security, lighting, parking, access control, receiving and distributing cargo, and treatment of high-value cargo.

73. _____. Justice Institute. Port Security Study for Wilmington, Delaware. Prepared for the U. S. Department of Justice, Law Enforcement Assistance Administration. Arlington, VA: Westinghouse Electric Corporation, January 1973.

Assesses the security of the Port of Wilmington and provides recommendations for improvement in the areas of Port police, physical security (fencing and lighting, cargo cribs, warehouse security, key control, planned construction), vehicle movement control, and cargo documentation control.

INDIVIDUAL AUTHOR INDEX

Individual Author Index (Continued)

Individual Author Index (Continued)

TITLE INDEX

Title Index (Continued)

Title Index (Continued)

Title Index (Continued)

SUBJECT INDEX

Subject Index (Continued)

NOTE: Most bibliographic entries indexed to broad categories (e.g., Planning/Design) also discuss more specific design concepts (e.g., Access Control) and may not herein have been crossindexed as such.

END