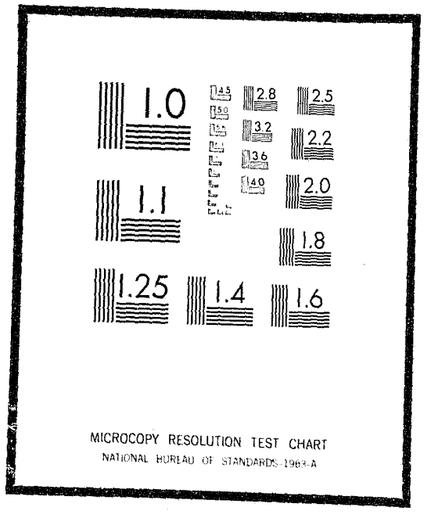


POLICE FACILITY SECURITY

VOLUME I

Prepared for

California Council on Criminal Justice

and

San Francisco Police Department

by

T. P. Chleboun

J. L. Sullivan

REPORT NO. 71-SSO-004

August 1971

GTE SYLVANIA SECURITY SYSTEMS ORGANIZATION
P. O. Box 188
Mountain View, California 94040

ABSTRACT

This report addresses the problem of security of police facilities. Methods and materials have been researched, and recommendations are offered.

FOREWORD

The staff of GTE Sylvania, Electronic Systems Group - Western Division, Mountain View, California wishes to thank all the persons who have contributed substantially to the research and development of this study report. Many individuals in each of the facilities referenced in this study were interviewed and all were extremely cooperative and helpful. Their generosity and cooperation in sharing their experiences and opinions materially assisted in the successful completion of this study.

The continued advice, guidance and recommendations of the Advisory Committee, created for this study, are greatly appreciated, and we wish to specifically acknowledge the neighboring police and sheriff's office representatives from Marin County, Richmond, San Rafael, Menlo Park, Frement, Alameda, Berkeley, San Jose, Vallejo, San Mateo, Oakland and Walnut Creek. We sincerely hope that they benefited as much from their participation as did the study group.

Details concerning past, present and future architecture and city planning as related to the San Francisco Police Department were unhesitatingly provided by Mr. Clement Mullins, San Francisco Bureau of Architecture, and Mr. Peter Groat, San Francisco City Planning. In addition, Mr. Marion Varner of Varner Associates, a recognized architectural designer of modern police facilities, contributed significantly to the discussion of security as it relates to newly planned facilities.

The task of visiting each facility and the resultant collection and collation of related details and drawings was performed in an outstanding manner by San Francisco Police Department Officers Michael Kemmitt and William Walsh.

Our thanks to Captain George Sully Jr., Commanding Officer of the Planning and Research Bureau, for his assistance as Moderator of the Advisory Committee meetings, and for his administrative support and personal contributions, based on his familiarity with many of the past situations concerning the various facilities.

During the initial phases of this study, questionaires were sent to the heads of law enforcement agencies of fourteen (14) representative cities throughout the United States. These questionaires were penetrating in nature, and required answers which could be

considered self-critical. The response was excellent, and we wish to commend everyone for being forthright, honest and cooperative.

In conclusion, we wish to express our sincere thanks to Chief of Police Alfred J. Nelder, who provided us with his counsel, cooperation, and continued encouragement. To Deputy Chief of Police Donald M. Scott and Supervising Captain Jeremiah P. Taylor (also Deputy Project Director) our thanks for their constructive criticism, advice and suggestions, which are reflected in this final report.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

SECTION 1

INTRODUCTION

This report is a result of a jointly funded (California Council on Criminal Justice/San Francisco Police Department) study for determining cost-effective measures to be used in securing police facilities against attacks aimed at destroying property and/or killing or maiming police personnel.

The study results are given in two volumes. This report (Volume I) discusses common vulnerabilities and specific ways in which to negate them. The results herein can be applied in whole or in part to any police facility. Volume II is published solely for distribution within the San Francisco Police Department, as it applies the recommendations of Volume I to each specific police facility within San Francisco.

An Executive Summary is given in the section following this Introduction. The Summary in turn is followed by Section 3 which discusses the organization of the study program and the manner in which the program was conducted. Various data were collected pertinent to threats and incidents which were perpetrated on police facilities in the past. These data and the results are given in Section 4. Section 5 uses these data to determine threat characteristics and vulnerabilities, and the requirements of a security system designed to negate threat effectiveness in exploiting the vulnerabilities. Section 6 discusses the various techniques used in security system engineering, and selects specific techniques consistent with the previously identified system requirements for application to police facility security. Section 7 summarizes the security system recommendations, and presents the subelement equipment costs.

If a police department is currently in the process of planning new facilities, Section 8, which discusses this planning process with emphasis on providing a secure facility, is of especial interest.

SECTION 2

EXECUTIVE SUMMARY

This report provides a detailed discussion of the various subelements of an integrated security system and their interrelationships. The requirements for a police-facility security system were established, and cost-effective security subsystems were selected for use in negating the threats. Some of the more salient recommendations are listed below.

a. Keep security monitor apprised of all activity in and around the facility.

b. Provide physical security to keep the public away from the outside of the building, and away from police vehicles.

c. Provide systems to detect intrusions across or through the perimeter fence, through gate areas, through all doors leading into the building, and on flat roof areas.

d. Provide an easily implemented scheme for identification of authorized personnel in areas surrounding the building.

e. Provide a method of easily installing detection systems and monitoring their outputs.

f. Deny places of easy concealment of explosives by keeping shrubbery and trash away from building for easy surveillance and the denial of good bomb implantation locations.

g. Deny visual access to snipers by filling in all windows except those required for surveillance. Surveillance windows should be of a bullet-resistant material.

h. Public access must be controlled at all times. The public should be allowed to enter the inner part of the facility only if escorted by an authorized person.

In general, all of the systems recommended are simple, reliable and flexible, consistent with the requirements of the application. For example, no need was identified for the use of a sophisticated volumetric detection system. The majority of detection devices in the facilities will be magnetic switches and beam-breakers - reasonable in cost, easy to install and to maintain. It is further recommended, however, that the continuous-line vibration sensor be used to detect intrusions through or over the perimeter fence and on flat roofs.

The system recommended for transmission of the alarm from the detection device to a monitoring point provides for maximum flexibility and ease of installation. The detection device interfaces with a remote alarm transmitter which is simply plugged into the nearest AC power outlet. The AC lines, themselves, are used for the transmission of alarms. This means that there is no need to run wire from point-to-point, since existing power lines are being used. All that is required to relocate either the remote alarm transmitters or the Display is to simply plug it in at the new location.

Another system which is recommended assists in the discrimination of authorized from unauthorized intrusions. During the operation of the facility, there will be many "intrusions" created by entry of authorized personnel into the limited-access area surrounding the building. It is highly desirable from a standpoint of good area control that some method be used to discriminate these intrusions. The method recommended is to electronically monitor all intrusions into the area (over or through the fence or through gates). Any intrusions over or through the fence, of course, can be automatically classified as an unauthorized intrusion. Intrusions through the gates, however, must be discriminated. This can be done through a cooperative method. Each authorized individual is given a small coded transmitter. The codes on the transmitter can be easily changed from day to day. Since a long-wire antenna can be looped around the building, the transmitters can be quite simple since they only have to transmit a distance of a few feet. An authorized intruder knows that he is being detected as he enters the gate. He also knows that within some predetermined time after the intrusion (of the order of 5 seconds), he must identify himself by depressing the button on his transmitter. If he does this and his transmitter has the proper code, no alarm will be generated. If, however, the intruder has a wrong code or no identification transmitter at all, then an alarm will be generated and displayed on the security monitoring console. The monitoring personnel then knows that an unauthorized person is in the limited-access area surrounding the facility and can take the appropriate action.

In addition to the above electronic equipment to assist the security monitor, there are a variety of physical security devices which are recommended for use in police facilities. These consist of fences, gates (remote controlled and manual), electric locks, bullet-resistant glass, physical and visual barriers, mirrors, and combination locks. These physical devices are very important to the operation of the overall integrated security system. They should be the first to be installed in any facility. This report details the recommended use of the above physical security equipment in the following sections.

SECTION 3

PROGRAM ORGANIZATION

The prime objective of this program was the determination of cost-effective measures which could be used to mitigate attacks upon police facilities. The program presented in the following paragraphs was designed to this end.

In order to provide any comprehensive recommendations from a study program of this nature, it is mandatory that a systems engineering approach be employed. The systems approach simply stated is that the problem must be fully defined, and all of the interactive subsystems must be identified. It is only after this preliminary work is done that solutions to the problem may be formulated, and that their impact on all subsystems may be observed.

A simple example of the systems approach might be given by considering the hypothetical activities of the owner of an inadequate lawn sprinkling system. For illustration let us say that the sprinkler system works fine except that the owner notices that one area of his lawn has not been receiving enough water. The owner may immediately rush to the hardware store and buy a sprinkler head which has a larger orifice in order to provide a greater flow in his problem area. After the owner installs the new head, he turns on the system to observe the results of his efforts. Much to his dismay, he discovers that indeed he is getting wonderful sprinkling action out of his new head, but because of the loss of system pressure through the large-orifice head all of the remaining heads are receiving not enough pressure to function properly. The only area of the lawn which is now obtaining enough water is his "problem" area.

The example illustrates a principle of systems engineering. Each of the sprinkler heads represents a subsystem of the overall system. The owner attempted to solve his problem without consideration of the impact of his solution on the operation of the entire system. It can be seen in this example that he optimized a particular subsystem (one sprinkler head) and actually worsened the performance of the entire system.

In the formulation of an effective security system it is necessary to place emphasis on the interaction of the subsystems constituting the entire system. Security subsystems can be identified as follows:

a. Deterrence
b. Detection

c. Delay
d. Communications
e. Response Force
   (1) Identification
   (2) Personnel Control
   (3) Capture

Each of these subsystems is uniquely important to the effectiveness of the overall security system. Emphasis is placed on each of these subsystems as a function of the specific requirements of the individual situation and the financial resources available for application to the problem. The interrelationship between the security subsystems is shown in Figure 3-1.

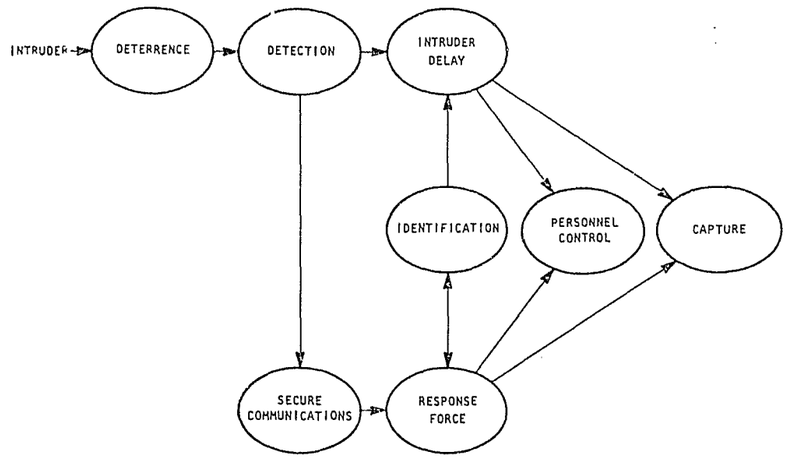


Figure 3-1 Security Subsystem Interrelationship and Time Sequence

For some security system requirements it may be necessary only to employ the use of an effective deterrent. If the potential threat probability is extremely low, it may be necessary only to provide a fence around the property. As threat probability increases and threat sophistication grows, it will become necessary to use more of the subsystem elements. The problem then becomes more complex and one must be conscious of the interaction of the various subsystem elements in order to provide a truly cost-effective security system. For example, there is no advantage in optimizing the detection subsystem if the response mechanism cannot respond fast enough to capture the attackers.

As can be seen in Figure 3-1, the security subsystems are related in a time sequence. The potential intruder will first encounter any subsystems which may exist to deter him from his mission. The deterrents employed can be of both a physical and a psychological nature. (Section 6 discusses each of these subsystems in more detail.) If the deterrents are not successful and the intruder continues his penetration, some means must be provided whereby his presence may be detected. It should be noted at this point that all of the subsystems can be implemented solely through the use of personnel; however, this is an extremely expensive way to operate a security system. One can achieve a cost-effective optimum system for a given set of requirements with some mixture of personnel and equipment. The detection mechanism in the vast majority of security systems is some type of mechanical or electrical system. This is true not only because of monetary considerations but also because humans have some severe restrictions when used as intrusion detectors. They have a limited sensing range; they fatigue quickly, and then rapidly lose their effectiveness.

After an intruder's presence has been detected, there are various functions which must be accomplished. First the alarm must be securely transmitted to the Response Force. The Response Force must, in turn, be able to identify whether the intrusion is that of an authorized or unauthorized individual. Depending upon the Response Force's reaction time, it may or may not be necessary to delay the intruder in order to effect a capture. If the intruder is identified to be an authorized person, it becomes incumbent upon the response force to enforce personnel control procedures.

There is a large variety of ways in which these security-system functions may be fulfilled. In order to evolve the proper system for a given situation one must thoroughly understand the limitations and applications of techniques and procedures to each security subsystem, and the impact on and interaction between the subsystems. Of course, it is mandatory that the situation itself be fully understood in order to determine the specific requirements which the system must meet.

The CCCJ/San Francisco police-facility security-study program was organized in a manner which would allow a determination of the requirements to which security system engineering could be applied for arriving at cost-effective recommendations.

A task-flow diagram of the program is shown in Figure 3-2. The first major task in the program was to gather data required for defining the vulnerabilities and threats to police facilities. The data were gathered from a number of sources. These sources included incident report reviews from San Francisco (the model city for the study) and 14 other major cities in the United States where police facility attacks have taken place.

In addition to the incident report reviews, data were obtained from the National Bomb Center and several other literature sources. The nine San Francisco company stations were reviewed in detail with respect to functions, procedures, staffing levels and facility design. Discussions were held with Mr. Marion Varner, of Varner Associates of Pasadena, California. Varner Associates is a noted architectual designer of functional, physically secure and esthetically pleasing police facilities. Mr. Varner contributed to a major portion of Section 8 of this report, which deals with the security of newly planned facilities. In addition to the previously listed sources, an Advisory Committee composed of high-ranking Bay Area police department representatives was established at the outset of the program for the express purpose of convening on a monthly basis to review and comment on the program as it progressed. The members of the committee provided additional data from their communities which were also compiled into the data base.

The data base was then used to determine the threats and vulnerabilities common to police facilities. These are identified in Section 5. Having identified the threats and vulnerabilities it was then possible to establish the security system requirements. The security system requirements were then used as a basis for formulating various systems to negate the threat. These concepts were then evaluated, to choose the most cost-effective approach for application to the complementary operation of each security subsystem.

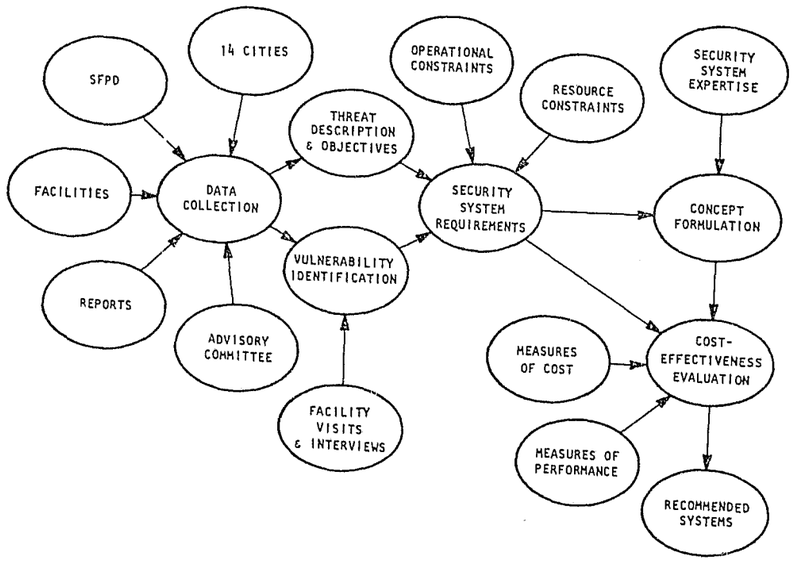


Figure 3-2 Program Organization Task Flow

SECTION 4

DATA COLLECTION AND ANALYSIS

The first series of tasks which was undertaken consisted of providing a data base from which a threat and vulnerability analysis could be conducted. It is essential in formulating an effective security system that as much information as possible about the threat be obtained. It would be most desirable to learn the complete nature of the threat, including the threat objectives, motivations, resources, technical expertise and most probable reactions to countermeasures. Of course, it is impossible in a real-world environment to learn completely of the threat's character and to be able to predict reactions with complete infallibility. It is incumbent upon the security system engineer, however, to assess the threat to the best of his capabilities. To this end, then, data were gathered from several sources, and subsequently used in identifying threats and vulnerabilities.

4.1 DATA COLLECTION METHODOLOGY.

This CCCJ/San Francisco-funded program used the City of San Francisco as the primary data source. The study was made generally applicable, however, through the use of an advisory guiding committee, the review of literature pertaining to the national problem, and the solicited participation of 14 major United States cities. Table 4-1 is a summary of the major data derived from each of them.

It can be seen that there were four major data sources: the San Francisco Police Department, the National Bomb Data Center (NBDC), Advisory Committee participation, and reports from the 14 solicited cities.

San Francisco - At the outset of the program, a questionaire form was prepared in order to serve as a checklist for obtaining data from the Advisory Committee. The only difference in the forms was that the Advisory Committee was not asked to fill out section 6, dealing with the details of their police facilities. This information was obtained only for the San Francisco precinct stations where specific implementation recommendations are being made in a separate report volume.

The questionaire form shown in Appendix A was used in obtaining and organizing the Incident Report and Facilities data for each of San Francisco's nine precinct stations, the Twin Peaks Communications Towers, and the Rifle Range. Nearly 200 incident reports were reviewed in detail. The results of the data collection and analysis from all of the

TABLE 4-1. DATA SOURCE SUMMARY

Data Source	Type of Data
San Francisco	Incident Reports
	Facilities Layout and Function Review
	Review of Security Memoranda
NBDC	Bomb Statistics
	Threat Character and Motivations
	Bomb Scene Procedures
Advisory Committee	Incident Reports
14 Cities	Incident Reports
	Security Procedures and Directives
	Police Fatality and Injury Statistics

various sources will be discussed in Section 4.2. In addition to review of incident reports and physical facilities, security suggestion files for each station were reviewed in order to assess the currently recognized security problems at each facility.

National Bomb Data Center (NBDC) - The National Bomb Data Center is operated by the Management and Research Division of the International Association of Chiefs of Police, under the funding of the Law Enforcement Assistance Administration of the U.S. Department of Justice. The purpose of the organization is to provide various services regarding explosive- and incendiary-device incidents. Among these services is the collection and evaluation of incident statistics. NBDC also publishes procedural bulletins on the development of bomb-incident policy, introduction to the devices themselves, handling, investigation, etc. The documents currently available were reviewed and assimilated into the data base.

Advisory Committee - An Advisory Committee was formed in the initital phase of this program for the express purpose of providing guidance and sequential progressive reviews of the program. This was implemented by holding monthly meetings, at which times the previous month's activities were presented for subsequent discussion.

The Advisory Committee itself was composed of high-ranking representatives from 12 Bay Area Police Departments, the San Francisco City Planning Commission, and the San Francisco Bureau of Architecture. At the initial meeting of the Committee, the 12

participating police departments were asked to provide data consistent with the questionaire format pertinent to their own departments. These data were subsequently pooled with those of the other two sources.

14 City Solicitation - A document titled Guerrilla Acts of Sabotage and Terrorism in the U.S. 1965-1970 lists some 417 attacks on police and their facilities. Fourteen cities in which these attacks occurred represented the majority of the incidents. These representative cities were Brooklyn, N.Y.; Chicago, Illinois; Cleveland, Ohio; Denver, Colorado; Detroit, Michigan; Fort Lauderdale, Florida; Los Angeles, California; New York, N.Y.; Philadelphia, Pennsylvania; San Diego, California; Seattle, Washington; St. Louis, Missouri; St. Paul, Minnesota; and Pittsburg, Pa.

To the police departments of these citites letters were sent which described this study effort and its objectives and requested that any pertinent data be forwarded to the San Francisco Police Department. Eight of the fourteen police departments responded with either incident reports/statistics or security procedures currently in use. These incident reports were all reviewed and added to the existing data base.

4.2 DATA RESULTS

A total of 352 incident reports were reviewed in detail during the conduct of this program. Two hundred fifteen incidents occurred in San Francisco, and 137 incidents were reported from either the Advisory Committee or the cities solicited. Of these 352 incidents, 42 were attacks on police facilities themselves, while the remainder represented attacks on policemen in the field. The scope of this study did not include the investigation of security for field operations, but these were included for the sake of interest. Table 4-2 is a summary of the total incidents reviewed for both facility and field as functions of the data sources. Since San Francisco was the prime data source for the study, the incidents for that city are further broken down in Table 4-3. It is interesting to note that approximately 10 times more field incidents occurred than station incidents. Of course, the incidents occurring at the station are of a very serious nature because of the potential of completely disrupting a police agency. It can further be noted that on the basis of the total of incidents a loss of life occurred in 10 percent of the station incidents as opposed to 3 percent in the field incidents. This indicates that the attacks on stations may be better planned. Many of the field incidents have been the secondary results of answering calls and/or making arrests. It can be seen, however, that personal injury or property damage incidents run approximately 27 percent for field operations, as opposed to approximately 16 percent for station incidents. Because of the fact that the threat is so variable it is felt that these statistics can be used only as general guides.

TABLE 4-2. SUMMARY OF TOTAL INCIDENTS REVIEWS

Data Source	Facility Incidents	Field Incidents	Total
San Francisco	19	196	215
Advisory Committee	2	8	15
City Solicitation	16	106	122
TOTALS	42	310	352

In addition to the derived data from above, various data and procedures from the National Bomb Data Center were reviewed. A summary of their incident statistics is included as Appendix B to this report. Various tables are presented which portray incidents as a function of geographic region, population group, suspected motive or intent, and types of devices and targets. Some of the more salient statistics are summarized as follows:

TABLE 4-3. BREAKDOWN OF INCIDENTS REVIEWED IN THE SAN FRANCISCO POLICE DEPARTMENT

Station	At Station			In Field		
	Total Incidents	Loss of Life	Personal Injury or Property Damage	Total Incidents	Loss of Life	Personal Injury or Property Damage
A Central	1			34	1	7
B Southern	7			9		1
C Southeast	4	1	1	26		5
D Mission	1			13		4
E Northern	1			29		9
F Park	2	1	8	36	2	12
G Richmond	1		1	8	1	3
H Ingleside	1		1	4		1
I Taraval	1			37		10
TOTALS	19	2	11	196	4	52

a. The highest number of incidents and greatest property damage occurs in the East-North Central Area (Illinois, Indiana, Michigan, Ohio, and Wisconsin).

b. Most incidents and property damage occur in cities with a population of 100,000 or greater.

c. In 52 percent of the incidents the motive was unknown. The highest ranking motive in the known instances was classed as juvenile vandalism, followed by racial, political and other protests.

d. Liquid incendiary devices proved to be most popular.

e. The most popular targets were commercial/manufacturing, followed by residences, educational institutions, vehicles, government facilities (nonpolice) and police facilities.

The above data are drawn from 764 incidents occurring over the period of 1 July 1970 through 31 December 1970. Additional incident statistics are given in Appendix B for 1188 incidents occurring over the period of 1 January 1969 through 15 April 1970.

The Guerrilla Acts of Sabotage and Terrorism in the U.S., 1965-1970 data are summarized by year for attacks on policemen in Figure 4-1. The data are taken over the period of January 1965 through September 1970. It can be seen that the number of incidents increased rapidly from 1967 to 1969. Since the entire year of 1970 was not available, a linear extrapolation was done which approximated 150 incidents for the year. The reason for the decrease from 1969 to 1970 is only conjectural but may be attributed to greater emphasis on firm police tactics, better training, etc.

The most complete data were those derived from San Francisco, the Advisory Committee and the 14-city solicitation. These data were placed in a summary matrix so that each facet of each of the 42 incidents could be readily observed. It should be noted that the individual perpetrating the incident is known less than 50 percent of the time. This was borne out in our own incident data and in those of the NBDC. It is quite difficult because of this to determine any detailed characteristics of the attacker himself. The next section discusses the threat, using the previously presented data as a base.

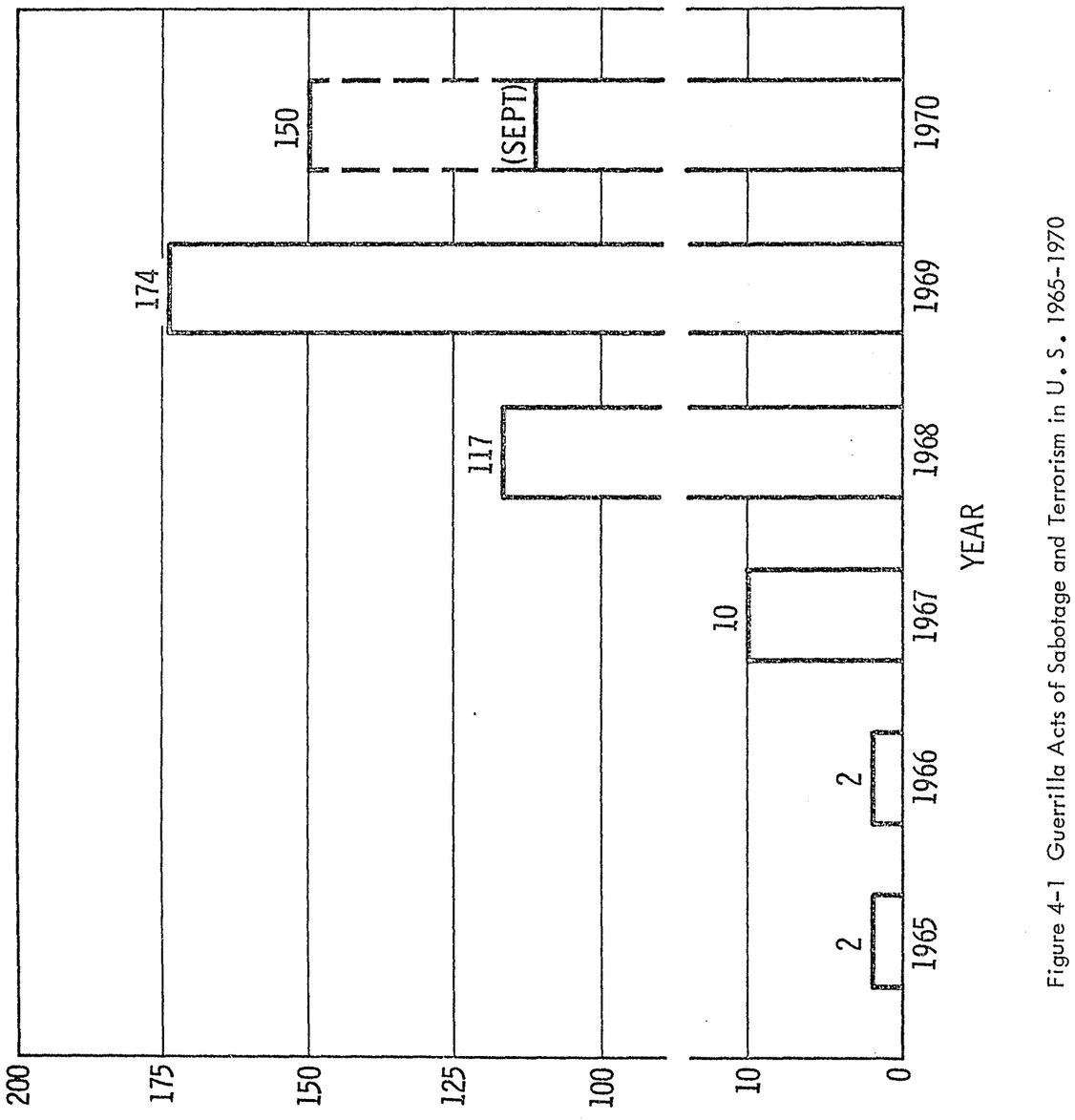


Figure 4-1 Guerrilla Acts of Sabotage and Terrorism in U.S. 1965-1970

SECTION 5

THREAT ANALYSIS AND SYSTEM REQUIREMENTS

5.1 THREAT DESCRIPTION.

5.1.1 General.

Most of the attacks on police stations, and police personnel in these stations, can be put into one of the three following categories: (1) bombings (both explosive and fire), (2) gun shots from outside the station (snipers), and (3) direct assaults on police personnel in the stations. Therefore, there will be three threat descriptions, one for each attack mode.

A comprehensive threat description will cover the following items:

a. Characteristics - This description provides such information as number of attacks, the attackers' political affiliations, background, what organizations they belong to, special training, etc.

b. Method of Operation - This description relates in as much detail as possible the common methods used in attacking stations.

c. Objectives - This descriptor identifies the objectives of the attack, e.g., killing or maiming of police personnel.

d. Skill Levels - This description gives information on the skill level required for various types of attacks, e.g., knowledge of manufacture and use of explosives.

e. Equipment Used - This description lists any equipment used by the attackers. Included are any tools, weapons, etc.

5.1.2 Bombings.

Of the 215 incidents which have occurred between 1965 and 1970 in San Francisco, 42 were attacks on police facilities. It was found that over 50 percent (24) were bombings, either explosive charge or fire.

5.1.2.1 Personnel Characteristics.

Actually very little is known about the groups that have engaged in such attacks. The primary reason for this is that they are very seldom apprehended. Of the incident reports studied, in only one instance is the name of the attacker known. His was an unusual attack.

He walked into a police station and tried to set fire to it. Of the remaining 23 incidents, two attacks were made by dissident Negro males and four attacks were made by dissident white males. Of the remaining seventeen incidents, nothing is known about the attackers. However, in two instances, the attacker(s) was probably a woman because the explosives were discovered in the women's rest room. A current Treasury Department study* concluded that only about one-third of all recent bombing incidents could be attributed to any specific cause or group. The breakdown for the known one-third was:

Campus disorder and student unrest	56%
Black extremists	19%
White extremists	14%
Activities in aid of criminal pursuits	8%
Labor disputes	2%
Religious difficulties	1%

5.1.2.2 Method of Operation.

There are two general methods used in emplacing the bombs. Each method applies to the type of building. One type of building is multifunctional, e.g., the Hall of Justice in San Francisco. Such a building can house jails, courts, etc., as well as the police facilities. These buildings usually allow unescorted access to many parts of the building. The method of operation is for the attacker to enter the building in a normal manner while carrying the explosive in a concealed manner, e.g., inconspicuous package. This package is left in such places as telephone booths, restrooms, trash containers, etc. The attacker then leaves the building in the normal manner. The explosive then detonates after some preset interval.

The other type of building is one which houses only the police facility. These buildings have very limited areas in which the general public can move at will. Usually the lobby is the only area in which the general public has complete freedom of movement. Attacks on these facilities take place during the hours of darkness. The bomb is placed by the attacker near the building, on the roof, or under vehicles in the parking lot and the attacker departs. The bomb then detonates some time later.

5.1.2.3 Objectives.

The purpose of all attacks analyzed was at least one, if not more, of the following: (1) kill or maim police personnel, (2) destroy property, and (3) embarass "the establishment'

*Development of Bomb Incident Policy and Procedures, The National Bomb Data Center.

5.1.2.4 Skill Levels.

The only skill required for the bombing incident is the ability to construct a bomb and provide a detonating mechanism (books describing these processes can be obtained at any public library). The detonating mechanisms have varied from lighted cigarettes to regular timing devices. Fortunately, a number of the detonating devices have failed to initiate the explosion. This might result from lack of skill on the part of the attacker.

5.1.2.5 Equipment Used.

The analysis has disclosed that no special or unusual equipment or tools were used in these attacks. The explosive used was, in most cases, dynamite or black powder, both of which are readily available. The detonating devices were simple timing mechanisms or cigarettes. The fire bombs were usually made of gasoline and soap.

5.1.2.6 Summary.

A summary description of the threat is: an individual or individuals with no distinguishing physical characteristics, without a special skill that required elaborate education or training, using equipment and material that is readily available to anyone.

5.1.3 Snipers.

Nine of the attacks were in the form of shots fired at police officers while they were in the police station or on the grounds adjacent to the station.

5.1.3.1 Personnel Characteristics.

Very little is known about the individuals who have fired at police officers because they are very seldom apprehended. In one instance, the attacker was a white male. He was not apprehended but was observed firing at the station. In another instance, the attacker was a Negro female. She seized an officer's gun and fired at him. Nothing whatever is known about the perpetrators of the other seven sniper attacks.

5.1.3.2 Method of Operation.

The method of operation is very simple, the attackers get close to the station with a gun and fire through the windows or shoot at police personnel moving between vehicles and the station. The only variation on this is that sometimes the attackers are in a moving car and other times they are not.

5.1.3.3 Objectives.

The purpose in all instances is to kill or maim police personnel.

5.1.3.4 Skill Level.

The only skill required is the ability to fire a gun. This "skill" is possessed by almost everyone within the United States.

5.1.3.5 Equipment.

The only equipment used is a gun, either pistol or rifle. These can be readily obtained anywhere in the United States.

5.1.3.6 Summary.

As in the case of the bombing threat the attackers are without any distinguishing characteristics, and they employ techniques which require no special skills and equipment that is easily obtained.

5.1.4 Assault.

There have been few assaults (only five) on police personnel while they are inside police buildings. Because there is a direct confrontation more is known about the intruders.

5.1.4.1 Personal Characteristics.

Although much more is known about individuals who engage in such assaults, it is more difficult to generalize about the distinguishing characterisitcs because there is no commonality among them other than a feeling of antagonism toward the police and "the establishment." In three of the assaults, it was the act of a single individual. In one of the other two attacks, it was three motocycle gang types. In the last instance it was a group of Mexican Americans known as the Brown Berets.

5.1.4.2 Method of Operation.

The general method of operation is the same in all cases. The attackers entered the station and attacked police personnel engaged in the performance of their normal duties.

5.1.4.3 Objectives.

Here again the purposes were the same: the killing or maiming of police personnel, and the destruction of property.

5.1.4.4 Skill Level.

Absolutely no education or training is required for this type of attack. However, the leaders of the Brown Berets did have some training in paramilitary methods as well as political organization.

5.1.4.5 Equipment.

The equipment used in these attacks were fists, knives, rocks, sticks, etc.

5.1.5 Threat Description Summary.

A general description of all three types of attackers is that the attackers have few distinguishing physical characteristics. They have very little in common except an antagonism towards police, and use equipment, tools and materials readily available. They use obvious means of attack which require very little skill or training.

5.2 VULNERABILITIES

5.2.1 General.

When analyzing vulnerabilities it is important not to restrict one's thinking to vulnerabilities associated with past attacks. Therefore, the additional vulnerabilities that must be examined and negated are: (1) those which attackers have not exploited, for some unknown reason, and (2) vulnerabilities which will become attractive to attackers when prime vulnerabilities have been negated.

Also, it is imperative to not either underestimate or overestimate the threat. To underestimate the threat results in a system which will not provide the required degree of protection; and to overestimate the threat results in a system which is more expensive than necessary.

The vulnerabilities of police facilities discussed in the next section are considered in the light of observations of police facilities in various cities, and discussions with police personnel.

5.2.2 Specific Vulnerabilities.

Most buildings housing police facilities are extremely vulnerable to almost any type of attack. The major reason for this is that the buildings were designed and built before attacks on policemen and their facilities began. Buildings that have been designed and built within the last few years are less vulnerable to attack. However, much can be done to improve the security posture of all police buildings. This is discussed in detail in Section 6.

Windows, especially those on the ground floor, cause the building to be very vulnerable to bombing and sniper action. Bombs can be placed on window ledges. Flying glass resulting from the explosion can do a great deal of damage. Further, uncovered windows allow snipers to observe the exact location of police personnel.

Lobbies provide attackers with an opportunity to destroy property or to kill or maim police personnel. The lobby provides the major interface between police personnel and the public. Usually, the lobby is adjacent to the business office, which renders police personnel quite vulnerable to sniper fire from inside the lobby, and to injury from a bomb detonated in the lobby.

A large enough bomb placed against the wall of the building, or on the roof, can cause considerable damage.

Another area of extreme vulnerability is in the gasoline storage reservoir. A "firefly", a fire bomb made of metallic sodium and calcium carbide, dropped into the filler insert would ignite the gasoline and cause a large explosion.

Bombs placed in the parking areas under vehicles can damage property and injure police personnel.

Another vulnerability is the air entrainment system. Incapacitating gas introduced into the air entrainment system would have serious effect on all police personnel in the building.

Police personnel moving between vehicles and the building are vulnerable to sniper fire.

5.2.3 Summary of Vulnerabilities and Likely Targets.

- Police personnel
- Control of Public access areas
- Garage, maintenance and parking areas
- Roof
- Air intake vents
- Weapon storage
- Gasoline storage and pumps
- Record storage
- Communications
- Fire escapes
- Little-used portals
- External portions of station which allow relatively covert approach and easy, effective placement of bombs

5.3 SCENARIO OUTLINES.

Detailed scenarious will not be presented in this report. However, scenario outlines will be presented to the depth required to describe the method of attack and to generate system requirements which wlll negate the specfic vulnerability being exploited. It is possible to establish criteria by which the various scenarious can be ranked, thereby determining the most important scenarios. This will not be done, however, because all of the scenarios are considered important and measures should be taken to negate the possibility of any of these scenarios being executed.

5.3.1 Bomb Placed Outside of Building.

The attackers, probably under the cover of darkness, would surreptitiously emplace a homemade bomb with a timer against the building. Window ledges are likely places to put bombs. At some preset time the bomb explodes.

5.3.2 Bomb Placed Inside Building in Vulnerable Area.

The bomb is concealed in a package, in a woman's purse, or in a brief case. The bomb is then covertly taken into the building and left. Bombs have been left in telephone booths, waste containers, and rest rooms. The attacker leaves and the bomb explodes at some later time. Multifunctional buildings are especially vulnerable to this type of attack; however, a package concealing a bomb could be left in the lobby of a police station. The explosion would kill or maim police personnel in the business office.

5.3.3 Bomb Placed on Roof.

The attackers gain access to the roof of the building and emplace a bomb. On or near skylights are good locations for such bomb emplacements. The attackers may gain access to the roof from adjacent buildings.

5.3.4 Bomb Placed in Gasoline Storage Tank.

The fill cap is removed from the gasoline inlet and a bomb is dropped into the storage tank. A firefly bomb is the most effective kind of bomb to use for this application.

5.3.5 Police Personnel Shot Through Windows and Doors.

The attackers shoot at police personnel while they are inside the building. The attackers are outside of the building, and shoot through windows and doors. The attackers could be in moving vehicles, standing outside the police buildings, or in buildings in the vicinity of the police facility.

5.3.6 Building Entered and Police Personnel Attacked.

The attackers enter the building and assault police personnel inside the building.

5.3.7 Bomb Placed Under Police Vehicles in the Parking Lot.

This scenario is very similar to the scenario outlined in 5.3.1 except that the attack is directed at police vehicles instead of the building. Under the cover of darkness the attackers place a bomb under a vehicle and at some later time it explodes.

5.3.8 Incapacitating Gas Injected in Air Intake.

The attackers surreptitiously gain access to the air intake port and inject an incapacitating gas into the air entrainment system. This will render the facility completely vulnerable to any type of attack because the personnel are helpless.

5.3.9 Personnel Shot as they Move Between Vehicles and Buildings.

This scenario is very similar to the scenario outlined in 5.3.5 except that the personnel are in a more exposed position.

5.4 SCENARIO VERSUS REQUIREMENTS.

After vulnerabilities have been identified and scenarios outlined, it is possible to generate generic security system requirements which will negate the identified vulnerabilities. The first step in the generation of system requirements is to determine what elements of security are required in order to negate the individual scenarios.

a. Scenario 5.3.1 Bomb Placed Outside Building

Requirements:

(1) Intrusion detection system across entrances to grounds.
(2) Illumination of the area around the station.
(3) Viewing device with which police personnel can survey the area without exposing themsevles.
(4) Physical barriers to deny anauthorized persons access to the area surrounding the building.
(5) Controlled vehicle gate.
(6) Perimeter system around entire area.
(7) Heavy mesh screen covering all vents.

b. Scenario 5.3.2 Bomb Placed Inside Buidling in Vulnerable Area

Requirements:

(1) Intrusion detection system across public entrance to building.
(2) Convex mirror in lobby to provide personnel with view of entire lobby area.
(3) Metal plate below counter to help contain explosion and decrease injury to police personnel.
(4) Bulletproof glass above counter. An amplifier system will be required to provide adequate communication between police personnel and the public. Because it is necessary for various objects to be passed between the public and police personnel, e.g., parking tickets, a port must be provided in the bullet-proof barrier. This then requires that a baffle be provided to deflect any objects thrown or shot through the port.
(5) Barrier between the counter area and the rest of the business office.
(6) Magnetic door switches on all outside doors.
(7) Electric locks on doors which handle a lot of traffic, whether police or public.

c. Scenario 5.3.3 Bomb Placed on Roof

Requirements:

(1) Device to detect the presence of an object or of people on the roof.

d. Scenario 5.3.4 Bomb Placed in Gasoline Storage Tank

Requirements:

(1) Tamperproof lock on inlet port.
(2) Key to be controlled by police personnel only.

e. Scenario 5.3.5 Police Personnel Shot at Through Windows or Doors

Requirements:

(1) Bulletproof barrier at counter in business office.
(2) Bulletproof barrier between counter area and remainder of business office.
(3) No outside windows except surveillance windows, which shall be of a bulletproof transparent material.

f. Scenario 5.3.6 Building Entered and Police Personnel Attacked

Requirements:

(1) Intrusion detection system across public entrance to building.
(2) Convex mirror in lobby to provide personnel with view of entire lobby area.
(3) Metal plate below counter.
(4) Bulletproof barrier at counter in business office.
(5) Barrier between the counter area and the rest of the business office.
(6) Magnetic door switches on all outside doors.
(7) Electric locks on doors which handle a lot of traffic, whether police or public.

g. Scenario 5.3.7 Bomb Placed Under Police Vehicles in the Parking Lot

Requirements:

(1) Intrusion detection system across vehicle entrance.
(2) Lights to illuminate the area around the station.
(3) Indirect viewing device.
(4) Fences.
(5) Remotely controlled vehicle gate.
(6) Perimeter system.

h. Scenario 5.3.8 Incapacitating Gas Injected into Air Inlet

Requirements:

(1) Same as requirements of g above.

i. Scenario 5.3.9 Personnel Shot as They Move Between Vehicles and Buildings

Requirements:

(1) Deny visual access to sniper.

The reader has probably realized that some of the requirements are applicable to more than one scenario. The scenario-versus-requirement matrix shown in Table 5-1 is included to show how the scenarios and requirements are related. Each system requirement is evaluated as to its effect on each scenario. A scoring of 1, 2, 3 is used; 1 is used when the requirement has very little or no effect on the scenario; 2 is used when the requirement will hinder the attacker in achieving his objective; 3 is used when the requirement will prevent the attacker from achieving his objective.

It is possible to calculate a score for each requirement and to then rank the requirements in order of their importance. This was not done as part of this study because each requirement is considered essential for a viable security posture.

TABLE 5-1. SCENARIO VERSUS REQUIREMENTS MATRIX

	5.3.1 Outside Bomb	5.3.2 Inside Bomb	5.3.3 Roof Bomb	5.3.4 Gasoline Storage Bomb	5.3.5 Sniper, Outside to Inside	5.3.6 Sniper, Inside to Inside	5.3.7 Vehicle Bomb	5.3.8 Gas in Air Intake	5.3.9 Sniper, Outside to Outside
Lock	1	1	1	3	1	1	1	1	1
Beam-Breaker	1	2	1	1	1	2	1	1	1
Convex Mirror	1	2	1	1	1	2	1	1	1
Metal Plate Below Counter	1	2	1	1	2	2	1	1	1
Bulletproof Glass	1	2	1	1	2	2	1	1	1
Barrier	1	2	1	1	2	2	1	1	1
Beam-Breaker	2	1	1	2	1	1	2	2	1
Lights	2	1	1	2	1	1	2	2	1
Indirect Viewing Device	2	1	1	2	1	1	2	2	1
Magnetic Door Switches	1	2	1	1	1	2	1	1	1
Electric Lock	1	2	1	1	1	2	1	1	1
Fences	2	1	1	2	1	1	2	2	1
Remotely Controlled Gate	2	1	1	2	1	1	2	2	1
Area Sensor	1	1	3	1	1	1	1	1	1
No Windows	1	1	1	1	3	1	1	1	1
Perimeter Detection System	2	1	1	2	1	1	2	2	1
Small Mesh Screen	1	1	1	1	1	1	1	2	1

5.5 SYSTEM REQUIREMENTS.

Section 5.4 discussed the security requirements for negating the nine scenarios. It is now possible to discuss overall security system requirements. These requirements will be discussed in the following seven categories:

a. Physical security and deterrence.
b. Intruder detection.
c. Alarm transmission.
d. Intruder delay.
e. Intruder identification.
f. Personnel control.
g. Response force.

5.5.1 Physical Security and Deterrence.

Physical-security and deterrence features of a system are defined as those feature which physically deny an attacker access to his objective. Included in this category are: locks, barriers which will contain bomb burst or bullets, barriers which deny visual access, fences, screens, etc.

a. Locks.

There are two major categories of locks to be considred: those which are opened by the individual desiring access, and those which are controlled by someone else and are opened after proper identification of the individual desiring access. The decision as to which type of lock to use should be based on such considerations as: (1) problems associated with keys and with coded badges, such as the problem of getting the key to proper people, (2) possibility of the key getting into the wrong hands, (3) the exposure of police personnel to sniper fire as they are unlocking a door or gate.

To summarize, there is a requirement to prevent unauthorized persons from using entry ways that are required by police personnel.

b. Barriers.

There is a requirement to protect police personnel from the danger of bombs and bullets. One type of barrier is that which cannot be seen through, and another is that which must provide police personnel with the maximum visibility possible. In the case of the complaint counter, provisions must be made for conversation between police personnel and the public, and also have feed-through capability so that such objects as parking tickets can be passed.

c. Fences.

Fences are required to deny the general public access to the area around the station. This fence should be strong enough to resist attempts to defeat it, and it should be high enough that it is not easy for a person to climb over the top. This fence should enclose the station area and also should channel pedestrians from the station boundary to the station entrance.

d. Screens.

It is required that all vents be covered with a mesh screen so that objects cannot easily be emplaced.

5.5.2 Intruder Detection.

Intruder detection equipment is required in order to detect the presence of intruders into certain controlled areas. The detectors of interest are point sensors, which are used when intruders enter portals, line sensors when an intruder crosses a perimeter, and area sensors when the activity within an area must be monitored.

a. Point Sensors.

These sensors are used to detect the opening of doors which are normally closed.

b. Line Sensors.

These sensors are used to detect intruders crossing a perimeter to gain access to a controlled area. These controlled areas are the lobby, and the station area. The entrance to the lobby must be monitored to alert station personnel of persons entering the station. There should be a fence around the station, with one vehicle gate and one pedestrian gate. There is a requirement to monitor the fence to detect persons attempting to penetrate the fence or to circumvent it. Also, line sensors are required at each gate.

c. Area Sensors.

There are two types of area sensors required. One is designed to detect the movement of persons on the roof of the facility and to detect the placement of objects on the roof. The other is a device to provide surveillance of the entire lobby area from the complaint counter.

5.5.3 Alarm Transmission.

Once a sensor has detected an intrusion, it is necessary to alert station personnel that an intrusion is in process. This requires that the alarm be transmitted to the business office, and that a display unit be provided which will display the alarm in such

a manner that station personnel are alerted to the intrusion and the location of the intrusion attempt.

5.5.4 Intruder Delay.

As defined here, intruder delay equipment comprises those elements of security which prevent intruders from escaping. Two of these are required. One is barbed wire on the fence, and the other is a lock on the lobby entrance door which when actuated locks the door and prevents people in the lobby from exiting.

5.5.5 Intruder Identification.

After an intrusion has been detected, it is necessary to identify the intruder(s) without exposing police personnel to danger. Therefore, there is a requirement for visual observation of the station area from inside the facility.

5.5.6 Personnel Control.

It is necessary for station personnel to enter the two entrance gates and to have access to the station area. Therefore, it is a requirement to automatically identify authorized personnel in the station area. It is necessary that this control be reasonably secure.

5.5.6 Response Force.

Once an intrusion has been detected or an attack on the station initiated, it is required to mount a response of a sufficient number of personnel with appropriate tools and weapons to subdue the attack.

5.5.8 General.

There are a number of general requirements that should be imposed on the selection of any item of the physical security system. These general requirements are discussed below:

a. Costs - The overall costs of physical security should not be higher than required to achieve a viable physical security posture. There are a number of "hidden" costs, in addition to the initial costs. These costs can be separated into two categories: fixed, and recurring.

   Fixed Costs

   (1) Equipment.
   (2) Installation.

   Recurring Costs.

   (1) Training of personnel.
   (2) Maintenance.
   (3) Facilities.

b. Human Factors - There is a requirement for a physical security system which is easy to operate and to maintain.

c. False Alarm Rate - A false alarm is defined as an alarm output from the system that was not caused by a valid intrusion. The problem with false alarms is that they require unnecessary response by police personnel. Therefore, the system false alarm rate should be as low as possible.

d. Aesthetic - It is important that police facilities do not have the appearance of an "armed fortress". Therefore, care must be exercised in the selection of physical security features and their installation. It is necessary that police facilities do not scare people away from them.

Section 6

SYSTEMS CONCEPT AND EVALUATION

The preceding section outlined the threat characteristics which are being dealt with, and the resulting system requirements needed to negate those threats. It should be pointed out at the outset that no security system is completely invulnerable and not subject to compromise. The object in formulating a security system is to provide enough deterrence along with effective detection, communication, and timely personnel control to deal with identified vulnerabilities in the most cost-effective manner. The interrelationship between these various subsystems was described in Section 3. Now that we have identified the threat, police station vulnerabilities, and the requirements which the security system must fulfill it is possible to formulate a system which meets the requirements.

For the sake of clarity, each of the subsystems will be discussed individually. Techniques and/or devices used which are applicable to each subsystem will be described along with their salient advantages and disadvantages. The system requirements for a particular subsystem will be reiterated, and a choice of techniques and/or equipment will be selected as being most appropriate for meeting the requirements.

6.1 PHYSICAL SECURITY AND DETERRENCE

Physical security is that part of security which is related to the physical configuration and/or structural integrity of the buildings and premises to be protected. This pertains to items such as locks, fences, mirrors, bullet-resistant glass, lights, and any physical structure designed to enhance security. Physical security and deterrence are discussed together in this section, since just the presence of some physical security measures will have a deterrent effect. Another measure of deterrence is provided if the potential intruder is aware of the face that some electronic security devices are being employed. Efforts, however, should be taken to prevent the potential intruder from knowing just what types of devices are being used, and in what locations, since this is knowledge he can use to attempt to compromise the system. Overt deterrence is that commonly associated with prisons -- high walls, fences an and barbed wire, armed guards, etc. Although this form of deterrence is most desirable from a security standpoint, there are social, political and economical reasons that a permanent overt system cannot be employed. This is not to say that they may never be employed. Certainly, in some circumstances, the strategic placement of armed guards around a police

facility may be one of the most desirable methods of preventing or controlling attacks upon police facilities. Overt deterrence, however, cannot be thought of as providing any long term solution to the problem of police security.

Most forms of physical security, however, are quite applicable to the protection of police facilities and will generally provide the maximum socially-acceptable level of deterrence. These items are listed and discussed below:

Fences
Gates (manual and remote-controlled)
Lights
Locks
Barriers

a. Fences.

Fences around the property line should be a dominant consideration in providing physical security. They act as a good deterrent and they keep the casual public away from the more vulnerable areas of the outside of the police building itself. In addition, they can provide a valuable delay mechanism for any authorized person with in the perimeter, and can also provide a base structure for the attachment of intrusion detection systems. Probably one of the more commonly used and cost-effective types of fencing is a chain link #2 mesh, #9 wire which is 8 feet high topped with 3 strands of barbed wire. All of the upright posts are buried in concrete.

It, at all possible, the fence should be installed around the property lines and in such a manner as to keep the public as far as possible from the sides of police buildings and any other critical areas. Most desirable is to have a fenced pedestrian walkway which leads into the reception lobby of the building. This provides maximum control of the public, and prevents persons from wandering aimlessly around the outside of the facility. The police car parking area, of course, should be within the police facilities and, therefore, also be completely fenced. When properly configured with regard to the particular installation, a fence will provide a good base in the overall security system.

b. Gates.

It does relatively little good if a fence is installed and the gate areas are not adequately controlled. The tendency to leave gates open because of the "burden" they place upon personnel is something which must be avoided if one desires a secure facility. Admittedly,

if one must get out of his car and unlock a gate to get to an authorized personnel parking area, it is time consuming, and this factor alone may prevent keeping vehicle gates closed. If they are not kept closed, however, the public is free to either walk or drive into these areas, which leaves the facility much more vulnerable.

In order to maintain security with an open gate, it is necessary to use a detection device in order to alert a security monitor that someone has entered. Some other means must then be provided to determine whether the person or vehicle entering is authorized. Such a scheme can be devised and is discussed in Section 6.4.2. An authorized-personnel-identification technique must be used in order to realize the full value of a fence system, if gates are to be kept open.

Remote-controlled gates will alleviate some of the operational "burden" of keeping gates closed; however, one must determine the best manner in which the gate is to be controlled. Some gates are controlled by another individual who, upon recognition of the person seeking access, will actuate the gate. This is a relatively expensive method, since it requires time from a human operator and he must have good visual access to the occupants of any vehicle. Another method of actuation is to use a key or card-reader system. When the person desiring access drives up to the gate, he can insert his key or card into the actuating device. The problems with keys are that they get lost, and eventually they may find their way into the hands of unauthorized persons (they can easily be duplicated). The card-reader device alleviates some of this trouble by allowing one to change card codes periodically in order to reduce the possibility of an unauthorized individual gaining access. Card readers and combination buttons, however, represent a good target for juveniles. They can easily disable such a device with a little chewing gum.

Probably one of the most effective remote gate-actuating schemes is the use of a changeable-code transmitter which is issued to each person that requires access to the area. The person seeking entry simply depresses the button on his transmitter. The transmitters can be made cheaply (less than $50) and if one got lost, the code for the entry system could easily be changed through the use of a plug-in module in the transmitters and the receiver. This type of system alleviates the problems encountered with the previously discussed actuating systems, and still minimizes the burden of operating a "closed-gate" perimeter system.

One-way turnstile gates, in some situations, may be used advantageously for controlling personnel. It is possible to hinder the hit-and-run type of individual who may enter a police facility, shoot at the officers and make his escape. A full-length one-way turnstile would be used by the public for gaining entry into the police facility. Once in the lobby area, his only way out would be through an electrically controlled door which is actuated by the clerk. This is an "instant capture" type of system. It is recognized that there may be sociological/political problems in implementing such a personnel control system, but that is one of the prices which must be paid for a highly secure facility. It is felt that the general threat characteristics exhibited today would not require such a stringent personnel control procedure.

c. Lights.

The vast majority of the threats against police facilities predominate in the evening hours. Darkness provides an excellent cover under which the bomber or sniper may operate. For this reason, it is recommended that all of the outdoor areas immediately surrounding the police building be well illuminated. The illumination should be installed in such a manner that the light shines out away from the facility. In this way, the deterrent effect of lighting is even greater, since the potential intruder is somewhat blinded. The illumination level should be a minimum of one foot candle, uniformly distributed throughout the area. This will provide sufficient light for visual surveillance even through the use of standard CCTV cameras.

d. Locks.

Good locks and lock control are always essential to good facility security. Most police stations, however, are manned on a 24-hour basis and the "front door" is always open. This sort of operation would not require extremely high-quality locks for the front door. There are areas, however, where quality locks and good control procedures must be followed. These areas are the "target" areas of the station. They include weapon storage, communication center, record storage, gasoline storage, fill ports, and normally locked doors into the facility such as a roof door.

Key control is a real problem and one which in most circumstances should be avoided by the use of combination or pushbutton locks. The combinations to these locks can be easily changed when there is a change in personnel. There are a number of manufacturers of good-quality dead-bolt combination and pushbutton locks.

Electric locks are convenient and effective for personnel control. These locks can be employed in areas such as the reception lobby for access to the inner portions of the station or on pedestrian gates for authorized-personnel control.

For additional control of the public, it is recommended that a reverse type of electric lock be installed at the front door to the lobby. Under normal conditions, the door would remain unlocked; but when the clerk pressed a button, it would lock the door. This would give the clerk an added time advantage if he saw an obvious threat approaching the station; or, if some individual (or group) makes threats from the lobby, the clerk may lock him in and take the appropriate action.

c. Barriers.

Security barriers are used in three ways:

(1) To deny access by physical impediment.
(2) To physically protect personnel.
(3) To deny visual access.

An example for the use cited in (1) is the walls of a safe. They are designed to provide maximum impediment to anyone attempting entry through them. The walls of the police facility serve this same function.

Barriers are also used to protect personnel from attack such as the bullet-resistant glass or plastic installed in the tellers' windows or over the clerk's counter in a police reception lobby. It is important in these types of installations that no vulnerabilities be left remaining such as a plywood panel at the bottom of the counter, an open space above the bullet-resistant transparent material, or an easily penetrated speaking tube or pass-through for papers. Incendiary or explosive bombs can be thrown over the bullet-resistant material, or bullets can be fired through a plywood panel, speaking holes, or access ports. Additionally, provisions must be made in such an installation for as unrestricted acoustic communication as possible. This can be provided through the use of a properly located two-way amplifier.

Physical security is also provided by denying visual access. If a gunman cannot see his target, he has little probability of hitting it. Three examples of the effective use of visual denial are: (1) slats interwoven in the outer perimeter fence to help preclude sniper activity against personnel on property, (2) the construction of a visual barrier approximately four feet behind the complaint desk in the reception lobby to preclude

firing at operating personnel, and (3) the visual and physical obstruction of all windows which are not absolutely necessary for surveillance.

f. Mirrors.

Convex security mirrors, such as those installed in retail establishments, can be used effectively in a police reception lobby. The physical configuration of many police lobbies denies the clerk direct visual access to all portions of the lobby. It is entirely possible to smuggle a time-delayed explosive device into the lobby, place it under the counter or in some other visually inaccessible area and walk out. Strategically placed convex mirrors will provide the clerk with the visual surveillance he needs. These devices are very reasonably priced and will go a long way in negating a very real threat.

Mirrors can also be effectively used at the sides of surveillance windows. They can be installed in such a manner that personnel within the building will be afforded a full view of the outside areas including the sides of the building itself.

In summary, physical security can be considered the first line of defense. When resources are limited, as they usually area, one should first concentrate upon establishing a good physical-security configuration. Other elements of the integrated security system can be added as additional resources become available.

6.2 INTRUDER DETECTION

There are a limited number of different phenomena that can be used to sense an intruder's oresence, a variety of sensing techniques for detecting those phenomena, a greater number of ways in which the detected signal is processed to make a decision, and a very large number of manufacturers who build everything from gadgets to high-quality sophisticated detection equipment for implementing a detection system.

How can man be described in terms of his measurable properties? He possesses a certain mass which has dielectric, attenuation and reflectivity properties, and he emits gases, heat, and a limited amount of radio frequency (RF) radiation. When he vocalizes or bumps into objects, he creats acoustic energy, and when he moves he displaces other objects in his path. If he is carrying out a mission, he may be transporting material which in itself may be detected. These are the prime phenomena which can be used to detect man and his movement through his environment. These phenomena and the sensor techniques used to measure them are summarized in Table 6-1.

Table 6-1. Man's Physical Phenomena and Associated Sensing Techniques

PHENOMENON	SENSOR TECHNIQUE
Mass	Pressure sensors
Emissions:	
Gaseous	Olfactronic
Heat	Passive infrared sensors
RF	Emission levels are so low that phenomenon cannot currently be exploited
Dielectric properties	Capacitance sensors
	Electrostatic field displacement
Attenuation properties	Active beam-breakers (visible light, infrared, ultrasonic and gamma radiation)
Reflectivity	Television (light
	Antenna loading (RF)
	RF and ultrasonic Doppler radar
Acoustic energy	Passive acoustic
Displacement of other objects	Switches
	Switch mats
	Foil
	Taut wire
	Seismic
	Stress
	Vibration
Material transportation	Magnetic (active and passive)

6.2.1 Detection Techniques

As was stated earlier, there is a large variety of devices currently manufactured which use one or a combination of these sensor techniques, with various signal-processing circuits which make the decision as to whether or not a man is present. In order to familiarize the reader with the generic types of detection systems which are available, each will be discussed. After the generic classes are discussed, the types applicable to police-facility protection will be identified.

For the sake of ease of applying these detection systems to various requirements, it is convenient to group the sensors with respect to the type of detection coverage they provide. To this end, the sensors are divided into four classes, which are: point coverage, perimeter or line coverage, area coverage, and volumetric coverage. Representative sensor types for each of these classes, listed respectively, are: switch contacts, beam-breakers, seismic sensors, and active ultrasonic systems.

Point-coverage detection can be used only when the threat can be predicted to gain physical access by entering through a limited number of portals. This assumes that the intruder will be constrained, by his lack of sophistication, by his need for haste, or by impenetrable physical barriers, to enter only through these portals. Point-coverage devices are very effectively against an unsophisticated intruder.

Perimeter- or line-coverage devices may be active or passive, and employ modulated or continuous-wave light, IR and sonic beam-breaking devices, balanced pressure systems, and differential seismic systems. These devices provide more coverage than the point systems, but are easily defeated if their existence and locations are known. As in the case of the point sensor, the line sensor cannot be considered as a sole candidate for providing security against a sophisticated threat. There may be specific applications, however, where use of the line sensor may be desirable.

Area-coverage devices include seismic, vibration, switch-mat, and capacitive systems. Seismic systems are very difficult to use indoors or in any areas of high activity because they are sensitive to vibrations caused by nearby traffic, rotating machinery, etc. The normal industrial structure acts as a very good propagating medium through which these seismic waves may be transmitted. Vibration detection systems (piezoelectric) can be mounted in a wall perpendicular to the vertical axis so that attempts to break into a vault or wall which require the expenditure of force in the horizontal plane will be detected. Capacitive systems are primarily used for protecting vaults and filing cabinets. A requisite to their use is that the surface be metallic, and it must be electrically isolated from ground. These types of devices can be circumvented by the sophisticated threat, but may be used to advantage in conjunction with other systems.

The volumetric-coverage systems detect motion, body effluents, or sound, in the volume of space to be protected. Because of the fact that these systems do protect a volume, the maximum amount of coverage is provided. It becomes very difficult for an intruder to enter the protected area, no matter what path he selects. This makes volumetric systems attrac-

tive for use in any high-security application. However, these systems are susceptible to more false-alarms than systems of lesser coverage. Prior to using a volumetric system, one must completely survey the area and eliminate the false-alarm sources for that particular sensing technique.

Table 6-2 shows the various types of sensors available, classified as to coverage type. A brief description is given below for each of these types of sensing techniques.

a. Point - Switches.

A large variety of types of switches, contacts and foil is available. Some of the switches can be mounted within door or window jambs, and others are mounted within the locking mechanism itself. Among the most sophisticated are the balanced magnetic switches which are nearly invulnerable to tampering or bypassing. These switches are generally considered to be reliable devices, and do a good job of protecting against portal entry.

b. Line - Taut Wire.

Taut wire systems are probably among the earliest security systems devised. These are normally configured into a fence in which the tension in a taut wire is monitored, and when it varies "significantly" an alarm is indicated. Strain gages, or even spring scale arrangements, can be used to monitor the tension. Although simple in concept, such systems are fairly complex to install because of the number of tension monitors required for a system of any magnitude and the critical tension adjustment which must be made for each line section (approximately 30 feet). The major problems are loading by snow, ice, animals, vegetation (loose tumble weeds and uncontrolled growth), and wide temperature fluctuations. If the tension adjustments are made too sensitive, wind will cause false alarms.

c. Line - Capacitance Fence.

A capacitance fence can be installed to measure capacitance either among several wires or between the fence and the ground. In either case, the presence of an intruder alters the dielectric constant and hence the capacitance.

In general, such systems require fairly elaborate automatic compensation for environmental changes. Radio-frequency pickup, lightning, snow, rain, vegetation, animals, birds, and ice are all serious problems.

Table 6-2. Sensor Techniques Classed by Coverage Type

COVERAGE	SENSOR TECHNIQUE
Point	Switches
Line	Taut wire
	Capacitance fence
	Active modulated and CW light beam-breakers
	Active modulated and CW IR beam-breakers
	Passive IR
	Gamma ray beam-breakers
	Active ultrasonic beam
	Magnetic
	Pressure
	Differential seismic perimeter
	Balanced transmission line
	Radar systems
	Continuous-line vibration sensor
Area	Seismic
	Vibration
	Stress
	Switch mats
	Capacitive
	Adaptive continuous-line vibration sensor
Volumetric	CW Doppler radar
	Ultrasonic
	Antenna loading
	Acoustic (passive)
	Passive IR
	Magnetic
	Balanced light systems
	Olfactronic
	Television

These systems can usually be successfully used in an indoor environment, but their presence is easily detected and measures can be taken to circumvent their detection capability.

d. Line - Active Modulated and CW Light Beam-Breakers.

Visible-light continuous-wave beam-breaker systems have been in use for some time. Their use at this date is primarily limited to performing counting, actuation, and annunciation functions. Because of the visible light beam, their presence is fairly easily detected and can be avoided or compromised. Standard compromising techniques include the use of a separate light source that can be introduced into the receiver at close range. The intruder is then free to enter the main light beam behind his auxiliary source since it will keep the receiver from alarming. In the case wherein the transmitter and receiver are mounted together and a mirror is used to beam back the light source, all that is required to compromise the system is the introduction of a mirror closer to the receiver or, as before, the introduction of another light source into the receiver.

The modulated light source represents an improvement over the continuous wave (CW) sources since it makes compromising the system a more difficult taks. In these systems, the light source is interrupted at some fixed frequency and the receiver has a filter input that is sensitive only to the modulated source. As soon as the modulated beam is broken, the system alarms. In order to compromise such a system (other than simply avoiding the beam), it becomes necessary to introduce another modulated-light beam into the receiver. Most systems are not sensitive to the exact frequency required and may actually accept light-beam frequencies anywhere within the same order of magnitude. Compromising a synchronous system (a receiver sensitive to phase of the incident light) requires that the light source be sampled and used to drive another source in synchronism. This is more difficult to accomplish, but is within the capabilities of a sophisticated intruder.

e. Line - Active Modulated and CW IR Beam-Breaker.

The infrared beam-breakers operate in the same manner as the visible-light systems. They are available in both the CW and the modulated form. The primary advantage of the IR beam is that it does not project a visible beam, and its presence is, therefore, more difficult to detect. A sophisticated threat, however, may employ external means of detecting the beam and employ measures similar to those outlined above to defeat the system.

f. Line - Passive IR.

The passive IR system senses body heat or any difference in heat between the object and the surrounding environment. The major advantage of such a system is that it produces no emissions which might aid the intruder in detecting its presence. Such a device will generally have two adjacent fields of view which are continuously compared with each other. This is done in order to allow the system to adjust to a slowly changing IR environment. Environmental changes will be seen in both fields and will, therefore, cancel each other. If one of the fields of view senses an IR change and the other does not, then an alarm condition is generated. The optical bandwidth of such a device is 1.8 to 20 microns, and employs dual active thermistor bolometers as the sensing devices. The two fields of view are each 1° in azimuth by 4° in elevation, with a separation between the two of 2°. The sensing range can be made to be greater than 1,000 feet. These devices in small quantities are expensive ($4,000 to $5,000 each), which limits their application. This sensor, of course, also possesses the categorical "line" disadvantage and can be avoided if its presence and field of view are known.

g. Line - Gamma-Ray Beam-Breaker.

There are no known commercially available gamma-radiation beam-breakers available, but the sensing technique is mentioned here as a point of interest. The device uses a linear gamma ray source and a series of proportional counters to monitor the area between the source and the counters. An intruder absorbs a portion of the emitted gamma rays and in effect masks the proportional counter. The resulting lower average proportional count triggers an alarm.

A typical system employs a 500-foot long plastic tube filled with radioactive gas (krypton) which results in a 10-curie gamma-ray source. Proportional counters are located approximately 70 to 80 feet away at intervals of 10 feet along a line parallel to the source. The system detects presence as well as motion.

The chief problems associated with this technique are rain, snow, or animals, which also absorb gamma rays. The device presents a potential health problem and is not known to have been approved for use.

h. Line - Active Ultrasonic Beam.

Practical short-range ultrasonic vehicle detectors are currently in production for use in traffic control. The systems are very similar, in operation, to the visible-light

and IR systems. The major advantage for thier use in the traffic control function is their insensitivity to changing light conditions and the fact that much ultrasonic energy can be produced since a continuous AC power supply is available. The systems do not exhibit any major advantages over the IR beam-breakers for use in intrusion detection.

i. Line - Magnetic.

There are several magnetic techniques that can be employed for intrusion detection. In general, the techniques detect ferromagnetic metal, hence some metal, even if only the intruder's shoe nails, must be present for detection.

The geomagnetic technique (passive) has been the most frequently employed. The earth's magnetic field is locally disturbed by the presence of metal. If a piece of wire is placed on the ground and a piece of metal moved across it, a current is induced in the wire by the moving magnetic field disturbance that crosses it. The induced current is proportional to the metal object's velocity and size, and inversely proportional to roughly the cube of the distance between the wire and the metal.

Large scale variations in the earth's magnetic field occur regularly. To reduce the signal induced by such variations, the sense wires can be formed into a series of loops by periodically crossing the wires. If the area of each loop is roughly equal and there are an even number of loops, then the induced currents oppose each other and hence cancel out. The entire system can be buried to make its detection difficult.

The geomagnetic technique has to date been employed chiefly as a backup system, since its detection performance is dependent upon intruder speed, the amount of residual magnetism of the metal he is carrying, and the distance of the metal from the sense wire.

A man carrying a rifle at shoulder height walking stealthily can normally be detected by a system buried at a depth of 6 inches. Sector lengths of up to 400 feet can be achieved by careful loop placement.

Active magnetic sensing will be discussed briefly in the portion of this section dealing with volumetric devices.

j. Line - Pressure.

Pressure-sensing systems possess the advantages of presence detection, passive, operation, and relatively simple concept and operation. They are subject to degradation by snow or water accumulations, animals, low flying helicopters, and frozen ground.

There is a variety of pressure sensors including strain gages. air bellows, spring scales, pressure-sensitive substances (both solid and liquid) such as certain rare earths of the lanthanide series whose electrical resistance varies with the applied pressure, etc. The problem is simply to measure the weight variation over a given surface contributed by the presence of an intruder. Substantial improvements have been made in the last several years in the development of low-cost air-mattress-like matting and pressure tube devices that can be configured in a perimeter system. The basic limitations are in the breadth of coverage and the sensitivity required to detect an intruder who spreads his weight by using the "snow shoe" approach. Shallow burial is normally possible.

The Westinghouse "Periguard" system employs two parallel hydraulic lines buried approximately five feet apart. The two lines are monitored by a differential pressure transducer. Gross environmental changes will affect both lines equally and will, therefore, be canceled by the differential monitoring scheme. When an intruder approaches the system, he introduces an imbalance in the system and causes an alarm. Disadvantages of the system are its expense and difficulty of installation.

k. Line - Differential Seismic Perimeter.

There is no known producer of a perimeter system employing the differential seismic technique, but the system is mentioned here as a matter of interest. Sylvania has conducted some exploratory internal research and development on such a system, and the results appear to be promising. The technique uses two parallel strings of seism-sensing geophones, which are buried, or simply placed on top of the ground. The geophone outputs are connected in such a way that one string has phase opposite that of the other. The signal is fed into a differential amplifier and comparator, and through signal-processing circuitry to an alarm threshold. The system works in a manner similar to that of the balanced pressure system in that gross environmental effects are canceled since both strings of geophones are effected in the same manner, thereby canceling each other. An approaching intruder will upset one string of the geophone array more than the other and will cause an alarm. This system has an advantage in cost (geophones are relatively inexpensive) and ease of deployment.

l. Line - Balanced RF Transmission.

The transmission-line intrusion detection system employs a terminated radio-frequency transmission line in a fence-like configuration to detect the presence of in-

truders within a narrow protected corridor. Sector lengths of 400 feet and fence heights of 7 feet are typical.

Radio-frequency energy is transmitted along the line toward the load, which is well matched; hence, little power is reflected toward the transmitter.

An intrusion into the region of the open-wire transmission line results in a large increase in reflected power, which is monitored and, if the change is significant, an alarm is generated. Rain, snow (unless extremely deep), ice, and small animals are not serious problems. The chief problems are with medium-sized animals, large birds, and uncontrolled vegetation.

The chief disadvantages of the system are its cost and its installation requirements

m. Line and Volumetric - Radar System.

Various radar techniques have been employed to detect the motion of objects on the ground. Of primary importance is the need to limit the field of view to a well defined region so that the system responds to intrusions only in the prescribed area. Toward this end, several techniques have been developed and used, singly and in combination. A monostatic radar system or one with a common antenna for transmission and reception can limit its field of view by the use of a directional antenna, range gating of a pulsed or FM radar signal (i.e., energizing the receiver only during the time interval corresponding to the echo interval of a specific range), or by special modulation of a pulsed or continuous-wave radio signal.

Radar systems, regardless of configuration, modulation, or antenna characteristics, are motion detectors. The signal produced by a moving target creates a Doppler shift (frequency shift) on the echo signal that can be separated from the clutter of signals echoed from fixed objects by filtering the echo signals and processing only those with the proper range of Doppler frequencies. The Doppler frequency is proportional to target velocity, and is a function of the geometric relation between the target and the radar transmitter and receiver.

The most common causes of false alarms for radar systems are motion of vegetation, fences, surface water, animals, birds, debris, rain, falling snow, hail, lightning, and transmitter frequency and power fluctuations. Performance can be substantially degraded by uncontrolled vegetation, snow build-up, and surface water.

Despite the complexity and the many sources of problems, bistatic radar systems have proven to deliver reliable all-around outdoor volumetric performance. In fact, to date, the only satisfactory volumetric outdoor systems in large scale deployment and operation are radar systems. A significant base of operational data is now available from deployed radar systems.

A single bistatic radar system can typically protect a region 100 feet in diameter and 15 feet high and average less than 1 false alarm per week on a year-round basis in severe climatic regions.

The obvious disadvantage of these systems is their expense. They are used primarily to protect military strategic operations.

n. Line - Continuous-Line Vibration Sensor.

Within the last year, a new form of sensor has been developed at Sylvania which appears to have major advantages when applied to intrusion-detection systmes. The sensor is a solid-state, small-diameter (less than 0.25 inch), flexible line which is continuously sensitive along its length to extremely small vibrations. This sensor has been employed quite successfully in military use, and shows great promise in further developments. Major advantages of the continuous-line sensor are its high sensitivity, its ease of installation and its cost (the cost of the line itself is less than $.50/ft.). Developments are currently underway at Sylvania to apply this sensor technique in a variety of ways to produce a high performance, low cost, outdoor perimeter system.

o. Area - Seismic.

Motion of a body across any surface creates a complex set of acoustic waves, which propagate along that surface. In particular, the vertical component of the Rayleigh wave has been found to be that most generally useful for detection systems. Both the amplitude and the frequency of the seismic wave resulting from motion of an object across the surface are functions of a large number of parameters including terrain, object size, speed, range, and the number and spacing of the seism-producing objects. The situation is complicated by terrain discontinuities in or near surface rock strata, and seasonal changes such as water-table level. Despite the many variables and the many sources of background noise such as wind, rain, cultural activity, animal movement, thunder, aircraft and microseisms, careful signal processing can and does result in highly selective security systems. On fixed sites with controlled terrain, many of the aforementioned

variables are substantially eliminated, or can be specifically identified and the signal discrimination task greatly reduced. Discrimination is based upon a combination of signal frequency, signal envelope variations with time, signal amplitude, and signal direction.

Much work has been done in designing and building seismic signal processors to be used in military tactical situations. Because of the high level of seismic "noise" found in an urban environment, however, these systems are not attractive. The exception to this is the use of seismic sensors in a perimeter system described previously where it is possible to cancel the majority of these seismic noise sources.

p. Area - Vibration.

Piezoelectric vibration pickups can be employed to detect attempts to gain forcible entry into a given area. They are classed as an area coverage device because they are sensitive to vibrations induced on the surface to which they are mounted. They are generally mounted so that their sensitive axis is in the horizontal plane, in order that normal earth and building vibrations (largely in the vertical plane) do not affect the pickups. Common employment is on the walls of a vaulted area where protection against forcible entry must be provided. If properly installed, these devices can provide a reliable means of detecting forcible intrusions.

q. Area - Stress.

The stress sensor is very similar to the vibration sensor, except that it uses piezoelectric strain gauges as the sensing element. The device actually senses minute dimensional changes in the surface to which it is attached and converts these changes in stress to resistive changes which are electrically measured. The system is designed to respond to large rates of change of frequency such as those induced by a human footstep. Frequencies greater than one cycle per second or slower than one cycle per minute are rejected. False alarms can be caused by anything inducing strains into the sensed surfaces at the proper rate. Among these would be rapid temperature changes, heavy winds, etc.

r. Area - Switch Mats.

Switch mats are primarily used to announce customers arriving in a retail store. The majority of these devices simply use the exerted pressure of the human footstep to close two metallic contact strips. Some recent work has been done in the development

of low-cost pneumatically actuated mats which could conceivably be used under standard carpeting instead of the usual carpet pad. The pneumatic system has an advantage in that it is a dynamic device and senses only the rate of change in pressure. This means that furniture, cabinets, etc., can be placed anywhere on the surface and will be automatically compensated. The new mats can be made very sensitive to any additional load. The system appears to be reliable. These pneumatic mats are not currently marketed as a mass item, but are available on special order. The mats are designed only for indoor use, although switch strips are available for outdoor use.

s. Area - Capacitive.

The capacitive device is used to detect a change in capacitance between any ungrounded metal surface and ground. When an intruder comes near or touches the metal object, its effective capacitance is changed and the system will cause an alarm. These systems can be made to be fairly reliable for use in an indoor environment. They have a further advantage in the fact that they are self-protecting. An alarm will be generated if there is excessive capacitance drift (as would be experienced in attempts to bridge the system) or if the antenna wire is cut.

t. Area - Adapted Continuous-Line Vibration Sensor.

The previously discussed Continuous Line Vibration Sensor can be adapted to operate as an area sensor. This is done by simply allowing the sensor line to act as a support of some flat material. Anyone walking on the material or throwing objects on it will set up a vibration in the cable and cause an alarm to be generated. The details of implementing such a system are further discussed in Section 6.2.2.

The prime advantages of an adapted continuous-line vibration sensor is that unlike a switch mat, the alarm threshold is continuously variable, so it can be easily adjusted to any degree of sensitivity, and the system is relatively inexpensive.

u. Volumetric - CW Doppler Radar.

This type of a device is commonly referred to as a "microwave system", as opposed to what is referred to as a "radar system" which is actually an antenna-loading device which will be discussed later in this section. The "microwave system" is a true CW Doppler radar and uses an FCC-approved operating frequency of 10.525 GHz.

The system consists of an RF source which beams microwave energy into a volume determined by the transmitting antenna configuration and metal structures in the imme-

diate area. If a moving object is within the area of coverage, it will reflect RF energy at the radio frequency plus the doppler shift (a frequency which is proportional to the object's velocity). This energy is received by the unit, where it is mixed with the original transmitted frequency, resulting in the retrieval of only the Doppler shift. If there is no moving object within the field, there will be no signal output out of the mixer, since all of the reflected energy received will be the same as that which was transmitted. The resulting Doppler-shift signal from a moving object is then amplified and processed to produce an alarm. These systems have come into prominence within the last few years as a result of improvements in microwave technology. There are several such systems that are commercially available for indoor applications.

v. Volumetric - Ultrasonic.

Volumetric ultrasonic systems are very similar in their operation to the microwave systems discussed above. Instead of using electromagnetic radiation, however, they use acoustic radiation in the propagation medium of air. The most popularly used frequency is 19.2 kIIz, which is above the normal hearing range. The transmitter and receiver transducers are identical and use either a magnetostrictive or piezoelectric means of generating the acoustic energy. They are placed in metallic domes that are resonant at 19.2 kIIz. The transmitter transducer(s) is energized and produces a 19.2-kHz tone, which fills the protected area by reflecting off the surfaces in the room. Reflected energy is picked up by the receiver transducer(s), where the acoustic energy is transformed back to electrical energy. If an object is moving within the area, the reflected signal will consist of the 19.2-kHz transmitted signal plus the Doppler-shift frequency caused by the object. The signal from the receiver transducer(s) is then mixed with the original 19.2 kIIz, and the Doppler signal is retrieved. This signal is then processed to discriminate an alarm status. A disadvantage of this system is that any movement of the propagation medium (air) will also produce a Doppler shift proportional to that rate of movement, thereby causing a false alarm. An advantage to the system is that the ultrasonic energy is easily confined by walls, doors or windows so as to produce a defined boundary of the detection volume.

w. Volumetric - Antenna Loading.

Antenna loading devices are commonly referred to as "radar" intrusion detectors. The system is composed of a monopole antenna which is directly coupled into the tank circuit of an oscillator. The antenna thus becomes an integral part of the tank circuit

reactance. When an intruder moves near the emission field of the antenna, energy is reflected back into the system, which changes the effective reactance of the antenna element. This reactance change, in turn, causes the oscillator to shift in frequency proportionally to the magnitude of that change. The oscillator frequency is monitored and when the frequency shifts beyond a predetermined threshold, an alarm is sounded. These systems operate around 400 MHz, which is not an FCC-approved use of that frequency. Typical coverage patterns of these systems are toroidal (monopole pattern) and the diameter is adjustable to approximately 50 feet. The pattern at this range is then approximately 20 feet high at its thickest point. The system is insensitive to movement directly above or below the antenna (in line with the antenna axis). Disadvantages of these systems are related to the pattern coverage and the radio frequency. The 400 MIIz readily penetrates most building materials used and, because of the circular sensing pattern, will sense outside the desired area if the system is adjusted to provide full coverage of a rectangular area. These systems, in general, are prone to higher false alarm rates than the "microwave" systems.

x. Volumetric - Acoustic (Passive).

Indoor acoustic systems enjoy very limited use because of their high false-alarm rate and their susceptibility to compromise. There are systems commercially available but they can be used only in specific applications. The most common systems reject frequencies below 1000 Hz in order to get away from noise being generated outside of the area to be protected. Low frequencies more easily penetrate structures, while the higher frequencies are reflected by them. Systems are available with automatic gain control (which makes the systems susceptible to desensitization by intentionally generating noise), or standard linear amplifiers. Such systems also provide a means of adjusting the number of times a threshold must be exceeded within a certain time increment before an alarm is sounded. Unless the system is installed in an acoustically isolated area, it is of little use against an intruder.

y. Volumetric - Passive IR.

All objects above absolute zero in temperature (-475°F) emit infrared (IR) radiation whose frequency is proportional to their temperature. It is this radiation, around 98.6°F, which is sensed to detect the presence of human intruders. Optics are used in the device to segment a volume of space into several lobes. The IR level over the lobe volume is averaged and establishes a reference point ot which a threshold is automatically adjusted.

If anything enters the pattern radiating a different level of IR (above the threshold setting), then an alarm is triggered. The term "passive" is applied, since the volume is not being irradiated by an infrared source. The sources are the room and the objects within it, including any human intruders. These devices are not sensitive to air turbulence (unless there are significant short-term temperature gradients established) and, because most building materials block IR, the unit's detection pattern will not penetrate walls. The system is sensitive to direct sunlight, animals within its pattern, and any short-term temperature-gradient changes.

z. Volumetric - Magnetic.

Active magnetic sensors have been developed for military applications; but these systems have not found their way onto the commercial market. The most commonly used sensor configuration is the induction coil. Thin-film flux-gate magnetometers have also been developed for military applications. These devices create a magnetic field and monitor any perturbation of that field caused by the introduction of a ferrous metallic object into it. Effective ranges of these devices are limited to a few feet. Because of its mode of operation, the intruder must, of course, be carrying ferrous metal in order to be detected.

aa. Volumetric - Balanced Light Systems.

Two types of balanced light systems have been developed, the continuous-wave and the modulated-light types. A representative system of the former is the Sylvania Photoconductive Intrusion Detection System (PIDS). The heart of the system is a pair of cadmium-sulphide photoconductive cells. These cells, located behind the hemicylindrical light-diffusers of the sensor units, normally detect stable incident light from a regulated light source. The detected light is the diffuzed resultant of light coming directly from the light source and indirectly from an infinite number of reflections -- from floor, walls, ceiling, and objects in the room. The cells are oriented so that the light intensity incident on all cells is approximately equal and symmetrical. The presence of an intruder causes unsymmetrical changes in the intensity of light reaching the two cells, and a difference signal is generated. If the amplitude of the difference signal exceeds a predetermined threshold level, adjusted to detect human intruders, an alarm indication is triggered.

A disadvantage of this system is its susceptibility to variations in ambient light conditions. All incident light must be well regulated. This precludes its use in rooms with windows or openings which will allow extraneous variable light to enter the protected area.

The Bagno Electronics MOST system (Modulated Optical Space Transducer) operates very similarly to the Sylvania PIDS system, except that it uses modulated light in the near infrared portion of the spectrum. The system consists of a 60-Hz tungsten-filament light source (a diode in series with one side of the AC line), camera(s) (the sensor head), and a control unit. The camera contains optics which encompass a 70° field of view and six silicon photovoltaic solar cells in the focal plane. Any change in the modulated light pattern received by the camera will result in an alarm. Because the system is sensitive only to the 60-Hz-modulated light, it will not respond to changes that are caused by unmodulated lights being turned on or off, headlights shining through windows, or clouds passing between sensor and sun. A disadvantage of the system is the relatively high level of power required for standby operation.

Neither the Sylvania nor the Bagno system is in current production, and there are no other known sources of balanced-light volumetric systems.

bb. Volumetric - Olfactronic.

The olfactronic systems electronically sense human-body gaseous effluents. Such systems have been developed for military field use, but there are no known systems available on the commercial market. If available, the systems would be relatively expensive, and would be sensitive to human activity surrounding the area to be protected, or to effluents which might be present in the normal heating or air-conditioning system. Such a system would be ineffective against a sophisticated intruder who sealed himself and an artificial breathing apparatus into a gas-tight suit.

cc. Volumetric - Television.

Television can be used in a number of ways for intrusion detection. The simplest is a camera continuously monitoring a prescribed region. Addition of remote control of zoom, pan and tilt can effectively increase target acquisition capability. A normally-off TV system which is activated by another kind of intrusion detector is effective in concentrating attention only when required, which is necessary in a large security system to reduce operator fatigue and reduce overall equipment complexity.

A number of schemes have been developed to use TV as intrusion detectors (commonly referred to as MTITV) rather than as an aid to intruder location as described above. The schemes have in common the measurement of a change in the background under surveillance by the TV camera. Thus, the motion rather than the presence of the intruder is measured.

TV moving target indicator (MTI) systems have problems in dealing with rapid changes in background lighting, which would preclude their use in areas which have translucent openings to the outdoors. TV systems are expensive to acquire, install, and maintain, but they provide a tremendous increase in human confidence by providing the guard with the capability of remotely observing the various protected areas.

Low-light-level television cameras would provide a further degree of protection, since an intruder could be observed in relative darkness. The intruder would not be alerted to the fact that he was being observed and immediate steps could be taken to approach him. Sylvania produces an LLLTV camera which uses a standard vidicon and will work in light levels as low as 10^{-4} foot-candle (equivalent to starlight) and as high as 10^{4} foot-candle (equivalent to direct sunlight). If one is considering the use of television in his installation, he should make the cost comparison between LLLTV and closed-circuit TV (CCTV) with lighting.

In general, it is felt that using television systems is not cost-effective. The systems would also require a relatively high level of skill in maintenance. There are specific instances which may, however, warrant a CCTV or LLLTV installation.

6.2.2 Applicable Techniques and Recommendations

The previous paragraphs discussed the various sensing techniques which are currently being employed for intrusion-detection systems. It can be generally stated that when a sensor system is made to cover increasingly larger areas the probability of false alarms increases, as does cost. This results simply from the fact that more "noise sources" are included in its increased detection pattern. In point of illustration, consider the two extremes of detection device types: point sensors versus volumetric sensors. The switch-type devices (point sensors) are extremely reliable, low in cost and virtually false-alarm free, while the volumetric system must include signal-processing circuitry to recognize a valid target, and can do this only within limited constraints, i.e., many noise sources have the same signal characteristics as a human intruder.

Volumetric systems are best used in facilities which may attract a sophisticated intruder and which are unattended for long periods of time. In this type of a situation the intruder, if he knows the doors all have switches and the windows all have foil, may choose to enter through the walls or roof. Switches and foil in this instance would be completely useless.

The greatest degree of coverage identified, for intruder detection for the protection of police facilities, is an area-type sensor for protection of roof areas, a line-type sensor for

intruder detection at the outer perimeter of the facility grounds, and beam-breaker devices at gates which lead into the area immediately surrounding the building. All other sensors can be of switch type (portal protection). The reason volumetric sensors are not considered applicable is because the probability is very small that an intruder will have the presence of mind, courage or time to penetrate a police facility by going through the roof or walls. The fact that the facility is a police station represents a rather formidable challenge, in the presence of which the potential intruder will be inclined to place himself in jeopardy for as short a time as possible. Through the data and threat analysis, it has been determined that what the policemen within a facility require is a method by which they can be continuously apprised of the status of various critical areas. Because of the fact than an intruder will not take the time necessary to penetrate the roof or walls, it is recommended that balanced magnetic switches be used on all doors into the building, and that foil be used on any critical window areas. It is anticipated that the use of foil will be minimal, since it has previously been recommended under Physical Security that all windows which are not critical for surveillance should be physically blocked up. All remaining windows required for visual surveillance should use a bullet-resistant material. Beam-breakers are more difficult to install, are expensive and require more maintenance and are, therefore, given third preference.

In order to deny access to critical areas, the area between the building and the property lines should always be a restricted area. Any unauthorized person entering this area should be immediately detected and the security monitor should be alerted. For this reason, entrances to this area must be controlled, and a perimeter detection system is required around the property line fence. Entrance (gates) can be monitored conveniently through the use of IR modulated beam-breakers. In line with a system discussed in Section 6.4.2, this detection system may actually consist of a pair of beam-breakers.

The choice of a perimeter detection system is a more difficult one to make. Most outdoor perimeter detection equipment, such as pressure and seismic systems, is not designed to work in a city environment. Beam-breaker devices are plagued by IR absorptions of fog, rain, or snow. Magnetic systems are expensive, and require a buried installation path about 5 feet wide. Capacitance fence systems are false-alarm prone in electrical storms, and a balanced transmission line or radar system is prohibitively expensive. There remain two systems which are applicable. These are the continuous-line vibration sensor, and the taut-wire system. Both systems are designed to be applied to the fence itself. The continuous-line sensor is by far the more desirable of the two, since it provides a signal output proportional to the physical stimulus placed on the fence. This allows one to easily establish an alarm threshold level to

preclude false alarms, yet reliably detect people either crawling over or cutting the fence. The taut-wire system on the other hand is a spring balance switch arrangement. Variations in temperature will cause the wire to expand and contract; therefore, its sensitivity varies with temperature. In addition, it is necessary to disturb the wire itself in order to be detected. The continuous-line vibration sensor senses any disturbance to the fence itself. Outer perimeter detection system recommendations would then be for a continuous-line vibration sensor, a taut-wire system, or a beam-breaker in that order.

Selecting a detection scheme for the roof area is also a difficult task. Again the majority of area sensors either are not designed to work in a city environment or are designed for indoor use only. One must be able to detect any human activity on the roof surface and, if achievable, should detect objects thrown onto the roof. Sensor systems are not required for steeply pitched roofs, since: (1) it would be difficult to lodge an object on it, and (2) an intruder would find an easier approach unless he were a steeple jack. Flat roof areas are recognized as problem areas. Seismic sensors cannot be used because of the high noise levels generated by traffic in their frequency band of operation. Stress sensors are designed for indoor use and are very expensive for covering an entire roof area. Switch mats and capacitance systems are designed for indoor use only. There are, however, two systems which could be adapted as roof area sensor which show promise: a continuous-line vibration sensor, or a flexible tape switch. Again, the continuous-line vibration sensor could be used simply by mounting the line along the top surface of two-by-fours laid parallel to each other about 4 feet apart. The two-by-fours and line would then be covered with some perforated material such as a stamped metal screening. The perforations would allow any differential pressures, which might otherwise build up as a result of wind action, to bleed off before exerting any physical force on the surfaces, and would allow normal roof draining. Such a system is depicted in Figure 6-1.

A tape switch mounted in this same way could also be used; however, the continuous-line sensor is much more desirable since it will put out a voltage proportional to the loading. The threshold setting for any particular installation can easily be adjusted. The tape switch on the other hand has only one threshold and that is established by the spring constant of the switch itself. It would be a rather tricky engineering problem to so design the system that wind loading would not cause the switch to actuate but a package or man would. After the system is installed, there is no way to adjust the point at which the switch actuates. This would have to be done with adjustable spring supports which would hold the perforated metal screening off

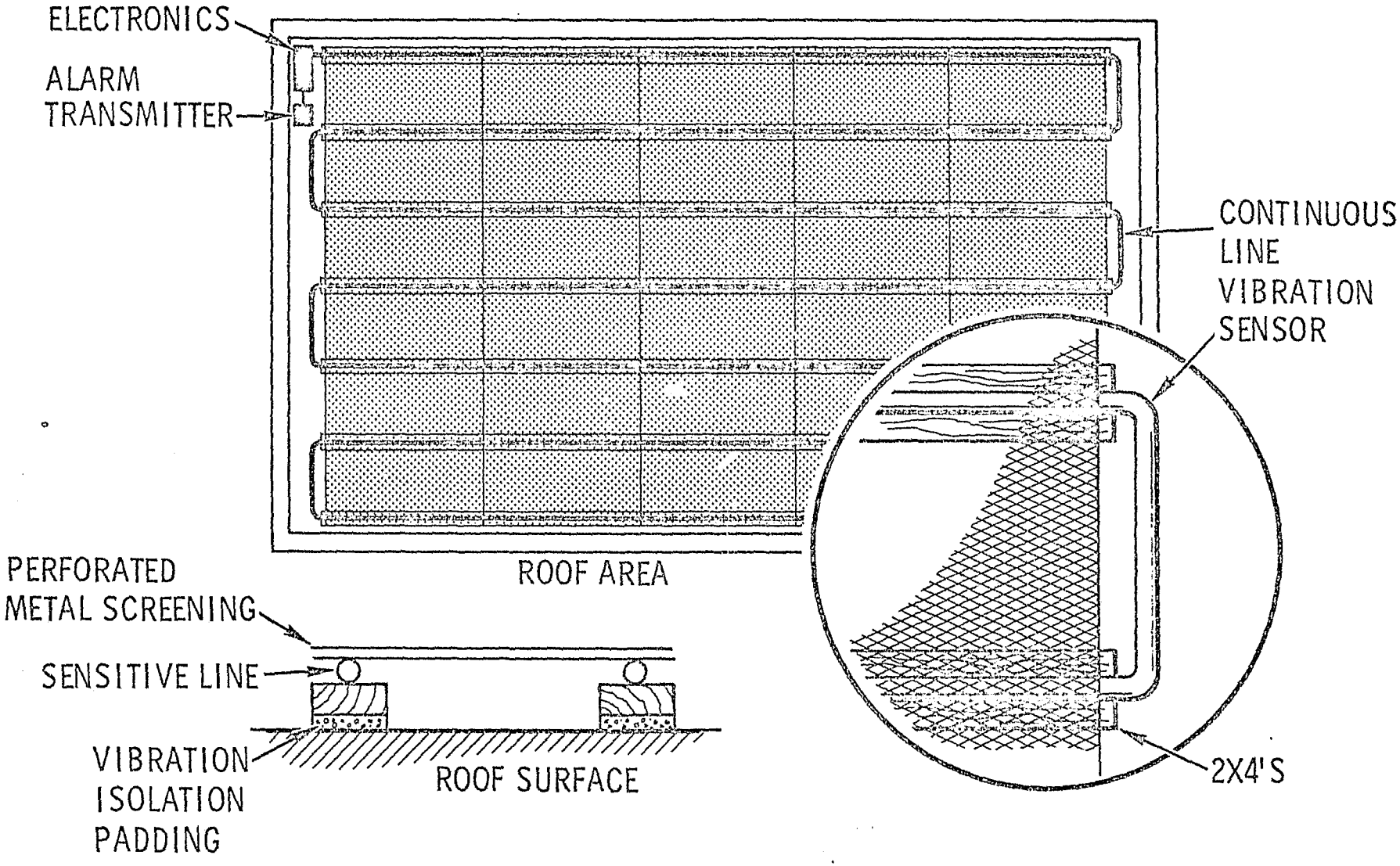


Figure 6-1 Roof Sensor System Installation

the surface of the roof. This, then becomes a greater design, installation and maintenance problems along with associated costs.

In view of the very reasonably priced materials comprising the adapted continuous-line vibration sensor system, it should be a very cost-effective system.

A summary of the various detection-device applications is given in Table 6-3. The order of preference is given where more than one type of device will work.

6.3 ALARM COMMUNICATIONS

After an alarm is generated, some means must be provided to securely transmit that alarm condition to the security monitor. There are tow primary methods which have been employed in alarm communications: radio frequency, and direct metallic contact lines. For a proprietary alarm system (one that is owned and operated by the police facility) there is another method of alarm transmission which is most attractive: a power-line carrier transmission system. Each of these approaches will be discussed in the following paragraphs.

6.3.1 Radio-Frequency Transmission

Radio-frequency transmission is more commonly used as an alarm transmission medium in military systems where long distances must be covered by easily deployed devices. The major advantage of such systems, obviously, is that there is no need for running long cables to a central monitoring facility. Early systems employed the use of various tone frequencies and their combinations to identify the alarm source and to provide a fair measure of protection in the generation of false alarms because of the transmission technique. The tones were used simply to modulate the particular (RF) carrier frequency used. With the advent of increasing emphasis on producing digital circuitry, the RF alarm transmission systems adopted the digital techniques. One could provide many unique identification codes, limited only by the transmission bandwidth and the time allocated for one alarm transmission. The RF digital systems are relatively immune to decyphering, but are still vulnerable to jamming. For this reason, emphasis was placed on short transmission times and relatively narrow bandwidths. This reduces the systems' vulnerability to jamming, but does not completely eliminate this susceptibility.

RF transmission is a relatively expensive technique, and need be applied only where no other technique will work, such as over long distances. There are now a few central alarm companies which are providing security service to groups of small towns, and are centrally locating their monitoring facilities. Alarms from each township report to a substation, where

Table 6-3. Summary of Detection-Device Applications

Protected Area	Sensor Device (in order of preference)
All entry portals into building	(1) Balanced magnetic switches (2) Properly concealed switch mats (3) Beam-breakers (IR CW)
Critical areas within building (weapon and record storage, communications, etc.)	(1) Balanced magnetic switch (2) Properly concealed switch mats (3) Beam-breakers
Roof	(1) Adapted continuous-line vibration sensor (2) Adapted tape switches
Outer perimeter	(1) Continuous-line vibration sensor (2) Taut wire (3) Beam-breakers
Gates	(1) IR modulated beam-breakers

they are encoded and transmitted to the central monitoring facility. This saves the cost of leasing long-distance telephone lines. Such installations at this time are relatively rare. It is safe to say that more than 99 percent of central alarm company subscribers are tied into a leased telephone line.

6.3.2 Metallic Contact Transmission

By far the most commonly used alarm transmission method is the metallic contact -- two wires which physically connect the protected area and the monitoring facility.

In central alarm station operations, there are two types of connection which can be made to the subscriber's premises. One connection is a direct line (analogous to a private telephone line), and the other is a McCullough loop (analogous to a party line). The McCullough loop is the most popular system, since the cost of the leased line is divided between 15 or more subscribers. In either case, when metallic lines are used some supervision of these lines is required. If the lines were not supervised, it would be possible to short or open the line and an alarm would never be received at the monitoring facility.

The most commonly used method of line supervision is to pass a direct current through the line, a resistor, and the normally closed contact set of the alarm device. The value of the current is continuously and automatically monitored. If the current exceeds certain tolerance limits (both high and low) an alarm is sounded. These tolerance limits are ±10%, ±20%, and ±40% for three classes of systems. A sophisticated threat, of course, would have no difficulty in substituting the proper resistance value in the line, thus breaking the connection to the alarm device simultaneously. For the vast majority of threats, however, this type of line supervision has been adequate. For higher-level line supervision, where one may expect an extremely sophisticated threat, complex digital systems have been devised wherein the monitoring station digitally interrogates the protected area, and the return response code is different each time, even though there is no change in alarm status. When there is an alarm condition, the protected area responds in another different digital code which is recognized by the monitor. The code is essentially changed for each interrogation/response cycle, but in a manner which is recognized by both units. These types of systems can be extremely difficult, if not impossible, to compromise.

In a proprietary system, it is still essential to provide some means of protecting the line running from the alarm device to the monitoring panel. The lines may be exposed to compromise during daytime operations. They could be compromised in such a manner that an alarm would never be sounded at the monitor, no matter what happened to the alarm device. Some electronics then, must be provided at the device end as well as at the monitoring end. In addition to that, the lines themselves must be run through conduit from each sensing device to the central monitoring area. Installation costs prove to be a major portion of the expense of an alarm system. Cable installation costs alone are $0.78/foot for surface-mounted conduit with a two-conductor wire pulled through. It would be far more economical if the line supervision, the monitoring station (alarm display) and installation could be accomplished through the use of a single system. A system through which this can be accomplished (and more) has been devised and is presented in the next section.

6.3.3 Power-Line Transmission

Power lines have been used to transmit information as well as power for many years. The power companies themselves use their lines to provide status information pertinent to the functioning of the power system. "Wireless" intercoms are sold in which all that is required to install the system is to simply plug the units into the nearest outlets in rooms in which they are to be used. The voice modulates a carrier frequency which is placed

on the power line and is detected and amplified by the other unit. One limitation of such units is that the sending and receiving units must be on the secondary of the same power transformer since the high-frequency signals are attenuated through the transformer. There are methods, however, for overcoming this problem. A typical police station will be served by one power transformer; therefore, the power transformer problem will generally not exist.

Sylvania has recognized the need for a system which can be used to economically and reliably transmit alarm information in small proprietary alarm systems. To that end, Sylvania is currently developing the CAT-20 carrier alarm transmission system. This one device will combine all the functions of monitoring, alarm verification, line supervision and installation in one system. This system provides a proprietary alarm system with an extreme amount of flexibility, since all that is necessary to move the monitoring station or to change the protected area is to simply plug the system into the nearest power outlet. A typical installation is shown in Figure 6-2.

The system comprises two parts: a Remote Alarm Transmitter, and an Alarm Display Unit. Both units contain internal battery supplies which automatically supply power to operate the system in the event of AC power failure. The system is designed to provide 20 independent channels of alarm information.

The function of the Remote Alarm Transmitter is two-fold. Its primary function is to securely interface the alarm generated by the detection device to the power line. A secondary but important function is to further provide a method by which the alarm situation can be verified. In the event of an alarm, the monitoring operator can selectively command the alarming Remote Alarm Transmitter to send acoustic data to the operator. The operator can then listen in to the remote area and detect the activity taking place. Because the Remote Alarm Transmitter employs line supervision, a failsafe feature, and tamper protection, there is no need to further protect the lines going into or out of the box or even the box itself. If the line leading from the detection device is either cut or shorted an alarm will be transmitted to the monitor. An alarm condition will also be generated if the AC cord is pulled out or if attempts are made to open the transmitter unit. Figure 6-3 is an illustration of the Remote Alarm Transmitter Unit.

The Alarm Display Unit provides the operator with an instant visual/audible display of alarms and gives him the capability to selectively listen in to any area in which a Remote Alarm Transmitter is installed. Figure 6-4 is an illustration of the modularized Alarm Display Unit. A separate receiver module is plugged into the main frame for each Remote

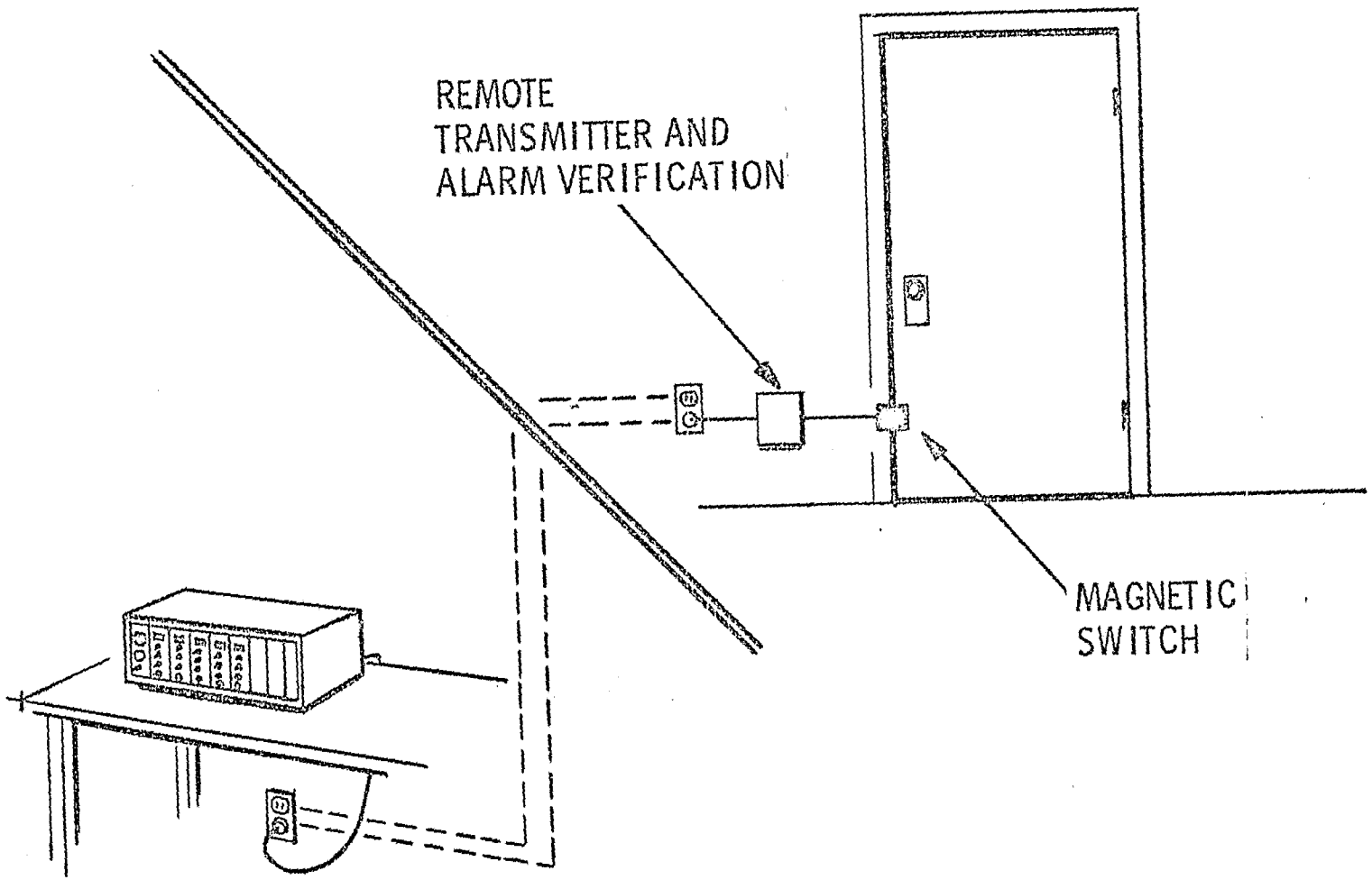


Figure 6-2 Carries Alarm Transmission System Installation

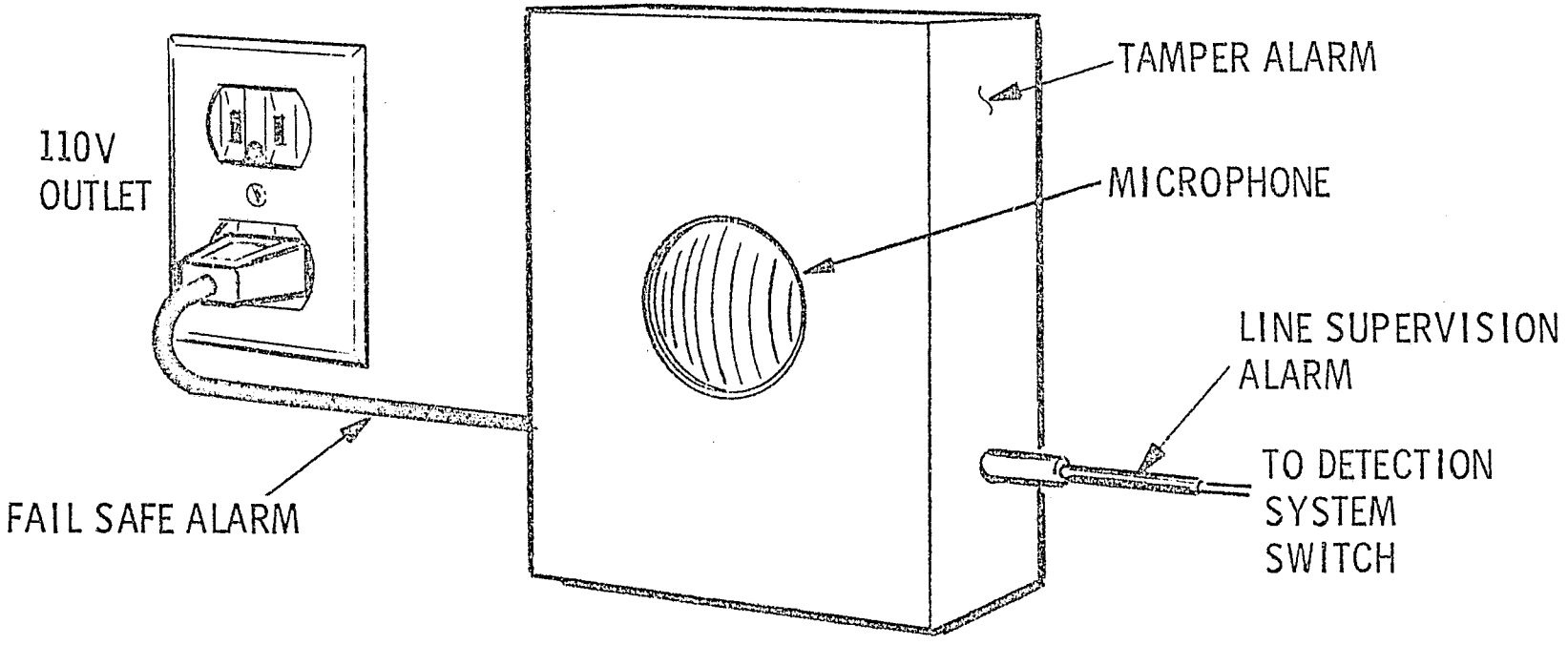


Figure 6-3 Remote Alarm Transmitter

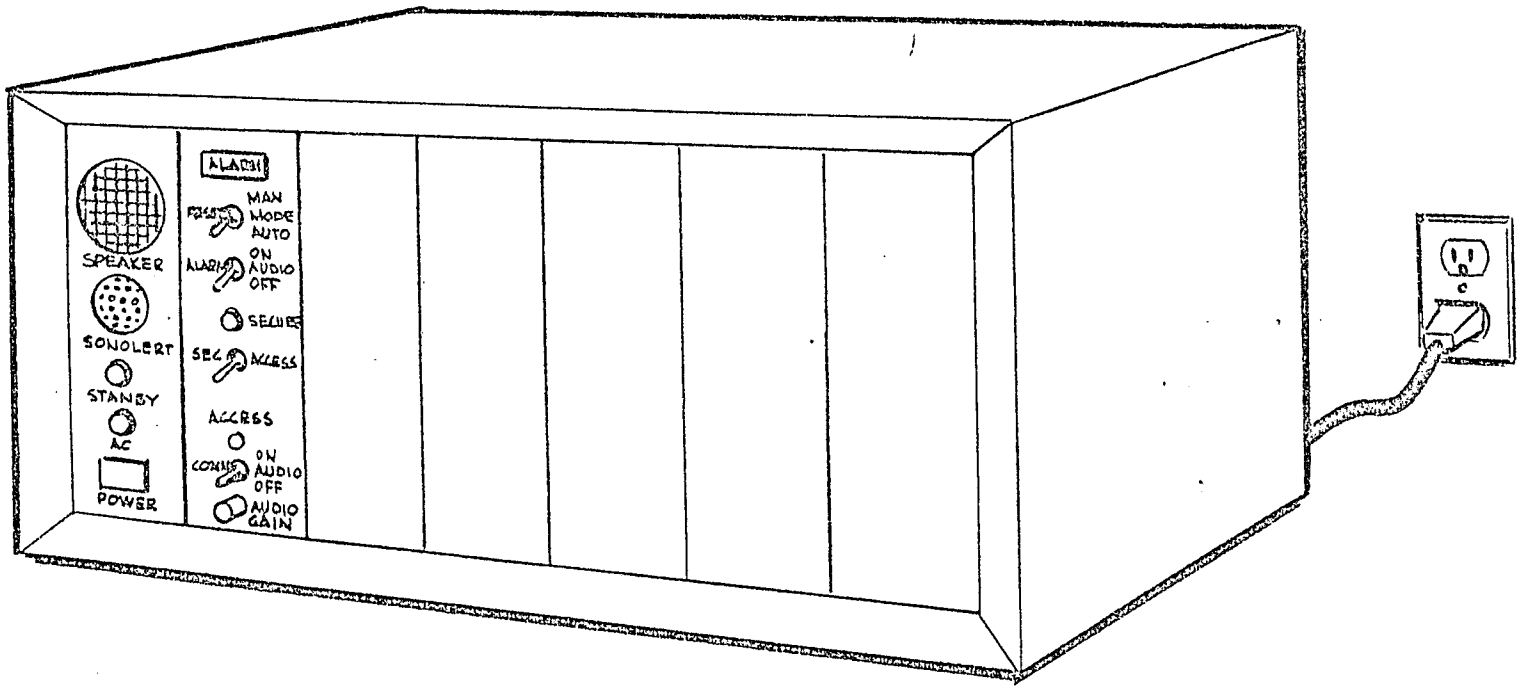


Figure 6-4 Alarm Display Unit

Alarm Transmitter deployed. The system is so designed that a total of 20 different channels may be used. One of the panels on the front surface of the unit provides all of the functions common to the units: a main power switch, indicators to indicate operation on AC or batteri a Sonalert for audible alarm annunciation, and a speaker for alarm verification.

Each plug-in receiver panel contains the functions peculiar to each of the individual channels. A red alarm light is provided to visually indicate an alarm from that particular area. A reset mode switch will determine whether the alarm must be manually reset (requiring operator interfacing) or will reset itself after the condition returns to normal. A switch is also provided to defeat the audio alarm if it is not desired for a particular monitor. The secure/access switch is provided for ignoring alarms from a unit. For instance, if a particular door is monitored only at nighttime, and during the day it is left open, the unit will ignore that alarm condition. When the secure/access switch is in the access position, an amber indicator shows that the system is not accepting alarms from that area. With the switch in secure position a green indicator shows that the unit is ready to monitor alarms. Another switch on the receiver module front panel allows the operator to command audio information from a particular Remote Alarm Transmitter for alarm verification.

The Remote Alarm Transmitter unit and Receiver Module are obtained as a pair. Each device is easily installed.

The CAT-20 system was designed to provide the maximum amount of flexibility, simplicity and reliability for proprietary alarm systems. The only additional hardware items required for a complete alarm system are the detection devices themselves.

6.4 RESPONSE AND CONTROL FORCE

The Response and Control Force is the single most important element in the integrated security system. The effectiveness of the entire security system is only as good as the performance of the response and control force. All security hardware, equipment and procedures are designed for the sole purpose of providing assistance to the response force. The physical-security items should act as a deterrent as well as assist the force in their personnel control responsibilities and provide maximum delay to a penetrating or retreating intruder. The alarm system should report intruder activity to the force at the earliest possible moment.

There are three subelements of the response and control force activity which have been touched upon, but not specifically addressed. Those elements are intruder identification, delay, and personnel control.

6.4.1 Intruder Identification.

In a police facility where unauthorized persons can and must be excluded from areas both outside and inside the building, it is essential that some means be provided for identification of persons penetrating those areas. The most difficult area to control is the area surrounding the building itself. Usually, procedures and locks are enough to control persons within the facility. The problem arises from the fact that areas surrounding the building support normal police operations and, as such, authorized personnel must have continuous access and egress capability in these areas. The control of these areas can be accomplished in basically two ways.

a. Provide an absolute gate control system and a detection perimeter around the entire facility.

b. Provide a detection perimeter around the facility and a means of discriminating authorized from unauthorized entries in gate areas.

In the first case, a guard stationed at each gate to control the traffic into and out of the areas would be interpreted as an absolute gate control system. This, however, is prohibitively expensive, i.e., a 24-hour, 7-day-week guard post costs in excess of $50,000 a year to maintain. Some other more cost-effective system must be formulated for absolute gate control.

Such a system might consist of a card- or RF-controlled gate on which the code can be easily changed in the event a card or transmitter is lost or there is a change in personnel. The card-reader device, as mentioned previously, is not desirable in this application because it can easily become the target of gum-chewing juveniles. In this event, the gates must be left open and guards must be stationed at the gates until repairs can be made. An RF-controlled gate does not possess this vulnerability and is, therefore, more attractive. A detection mechanism must still be provided on the gate itself to prevent intruders from climbing or cutting through them. This means that an alarm would be caused each time the gate were used by authorized personnel as well. In order to negate that alarm it would be necessary only to interlock the gate-actuating mechanism with the alarm device so that no alarm would be sounded if the alarm and gate were actuated simultaneously. It would be incumbent upon the authorized personnel using the gate to see that no unauthorized person or vehicle entered with them. This type of system would provide positive control of the perimeter through a normally closed gate system.

A similar type of control system which provides more flexibility is the type in item b. above. This type of system is a "normally open" gate system. A detection perimeter, RF-controlled gates, and some method of personnel identification, are the prime components of

the system. In this type of system, the gates can be kept open during the daytime when they are most often used, and closed at night to provide a further measure of security when most needed. The system can also be operated without any gates at all, but this places more burden on the response force, since they must respond to all unauthorized intrusions. If gates are kept open, even though they are thoroughly posted with "Authorized Personnel Only" signs, the public is bound to wander into these areas. If the monitoring operator has visual access he could effect a response through the use of an external public address system to warn the wandering intruder that he is in a limited-access area. Otherwise, he must send someone outdoors to investigate. For the sake of convenience, the public address response is more desirable. This type of response could even be automated through the use of a prerecorded tape. Whenever a perimeter violation occurred, the message would be played over the PA system.

The alarm system around the perimeter and at the gate area will notify the response force to determine whether the intrusion has been made by authorized or unauthorized personnel. It can naturally be assumed that if the fence itself is intruded upon, that it is unauthorized. If, however, the intrusion is through the gate then it could be either. Short of using full-time guards for the identification process, there are basically two ways in which identification can be accomplished. One method is direct or indirect (CCTV) viewing by a human operator; the other is an automated identification scheme. If direct visual access exists in a particular installation, one need not consider any other technique of identification. When the monitoring operator receives a gate alarm, he can simply visually identify the intruder. If, on the other hand, the operator does not have direct visual access (which will be true in probably 90 percent of the applications), one of the other two identification techniques must be used.

Identification through the use of CCTV is more or less self-explanatory. A CCTV camera would be mounted in such a position so that its field of view would cover the gate area. When a gate alarm was generated, the monitoring operator would look at his TV display to verify that the intrusion is an authorized one. If it is not, then he must take the appropriate response action.

Figure 6-5 illustrates the manner in which an automatic system for identification of authorized personnel would work for an "open gate" system. The drawing depicts a police station surrounded by a fence with two access ways into the rear parking lot. Double modulated IR beam-breakers are placed across the access way on each side of the building. The beam-breakers are used in each position so that the direction of movement can be determined automatically. Simple logic circuitry is used to determine whether the person or vehicle is going

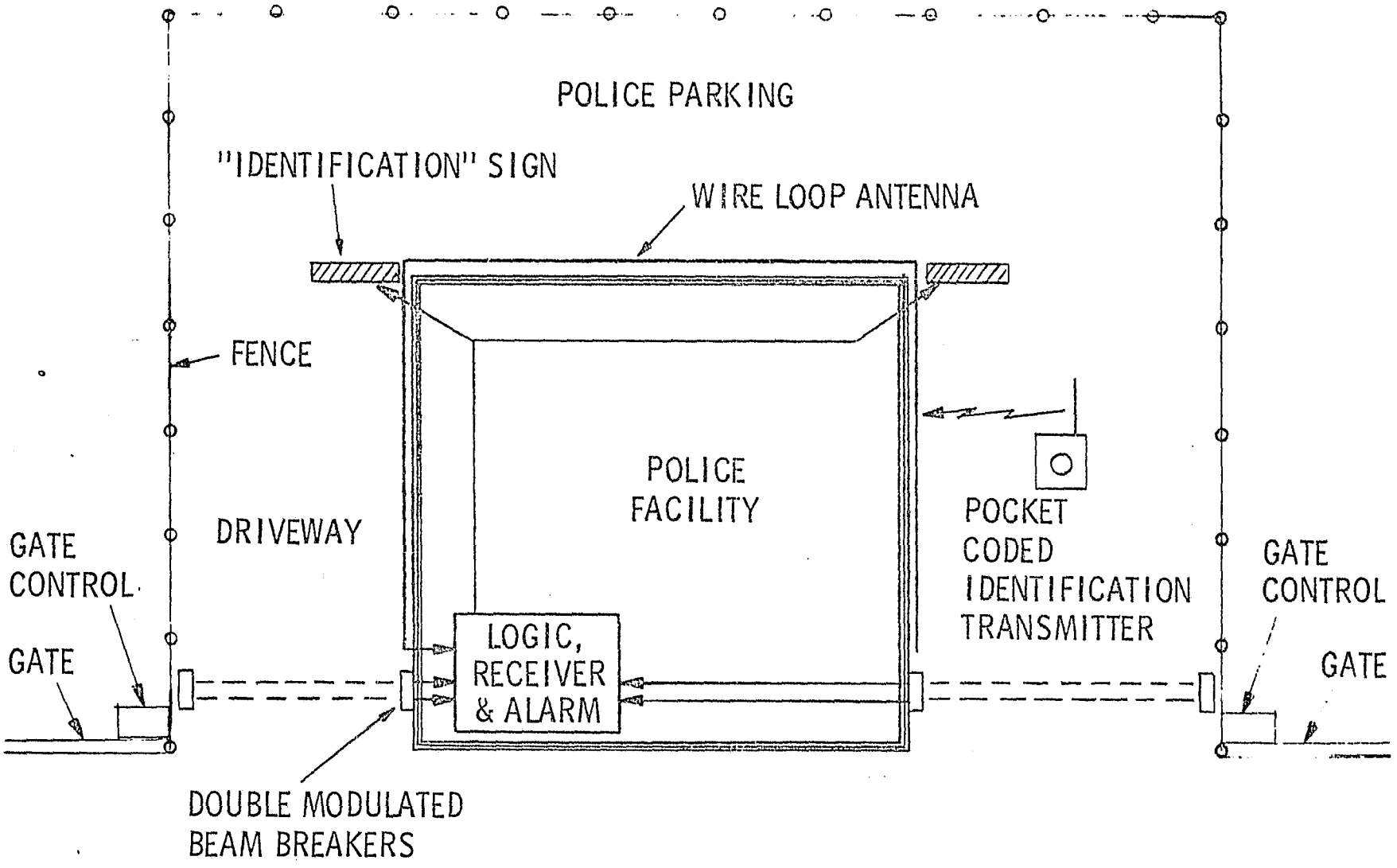


Figure 6-5 Automated Identifications of Authorized Personnel

out or in. If the movement direction is out, then no alarm is generated. If the movement is into the facility, then an "identification" sign flashes, or it can more simply be done through procedures, so that the intruder knows that he must identify himself within a predetermined time. Authorized personnel accomplishes this through use of a simple coded pocket transmitter. A loop wire antenna is used around the building, so the transmission must travel only a few feet. The codes on the transmitters can be changed easily through the use of a plug-in encoder. The code plugs are routinely changed periodically. The Logic, Receiver and Alarm unit generates an alarm if this coded transmission is not received within the predetermined time (approximately 5 seconds after the beams are broken). If the transmission is received within the proper time period, no alarm is generated. This type of system is less complex than a CCTV installation, and provides an automatic identification of authorized personnel. Since the transmission identification codes can be randomly changed, there is a very low probability that someone could select the right code even if he had one of the ID transmitters in his possession.

Table 6-4 shows a comparison between the video and automated identification techniques. The prime advantages of CCTV are that it allows one to assess the threat (number of intruders and weapons) and that one can periodically glance at the screen to observe any activity. The latter advantage is further enhanced (at a significant increase in cost) by adding remote pan, tile and zoom capability. Then too, however, one always runs the risk of a burned out vidicon if the operator accidentally points the camera toward the sun. The use of CCTV does not guarantee the proper identification of authorized personnel. Someone wearing a police uniform may have a high probability of being incorrectly identified as being authorized. In general, one must carefully assess the role in which he wants a CCTV system to serve before he commissions a costly installation which may very well not meet his requirements.

If the above system were used with electric gates (normally open during the day), the same identification transmitter would be used in the evening to automatically open the gates. This would be accomplished simply by throwing a switch from daytime to nighttime operation.

It is estimated that an identification system such as described above would cost approximately $4000 for the equipment (including 30 identification transmitters at $50 each). This would be comparable to the cost of a good-quality CCTV in an environmental enclosure with the TV monitor and alarm devices. If pan and tilt controls and a zoom lens are added, the CCTV cost will be significantly increased (by approximately $2000-$3000).

Table 6-3. Video Versus Automated Identification

	Advantages	Disadvantages
AUTOMATED IDENTIFICATION	• "Positive" identification • Low maintenance • Simple electronics • Automatic alarm for non-authorized intrusions	• Cannot directly assess threat
VIDEO	• Threat assessment • Discretionary visual surveillance	• Relatively high equipment and accessory costs • High maintenance (often and expensive) • Must be augmented by alarm device • Depends on visual recognition of authorized personnel

For the majority of installations, the RF identification system is the most cost-effective. The electronics are simple, positive identification is assured, and maintenance is less than that of a CCTV installation.

6.4.2 Intruder Delay

After an alarm is generated, it is necessary to determine whether it was actually caused by an intruder or by an authorized person. The verification mechanism for doing this at the outer perimeter gates was discussed in the previous section. Alarm verifications within the building can be augmented through use of the acoustic channel on the alarm transmission link (offered in Sylvania's CAT-20). It is further required that the intruder be delayed or impeded as much as possible in order to give the response force enough time to effect a capture.

The problem of implementing effective, reasonably priced intruder-delay systems is, for the most part, still unsolved. If one is in a tactical situation he may use lines of concertina, bamboo spikes, and caltrops, but these mechanisms are hardly applicable to a police facility. Any delay devices used must be esthetically pleasing or hidden, as well as functional. Exotic devices such as hidden fences which spring upright when an alarm is generated could be designed and fabricated but the cost would undoubtedly be prohibitive. The primary acceptable (from

both a cost and sociological view point) intruder delay system elements comprise fences, electric locks, and remote-controlled gates.

The outer perimeter fence and gates are a critical element in any intruder-delay system. The intruder, in penetrating a facility, will take his time as long as he believes his activities are undetected. For this reason, the alarm should not be used to automatically turn on floodlights, sound bells, etc., if one expects to capture the intruder. If a perimeter fence is topped by three strands of barbed wire, it does not represent a formidable barrier to penetration if the intruder has time. However, those three strands of barbed wire appear much more formidable when attempting to make a hasty retreat. Even if gates are kept open during normal hours, the gates themselves should exist, and it is very desirable to have them remotely controlled. The gates should also be topped by barbed wire. If the gates are open when a perimeter alarm is generated, they can be immediately closed to provide additional delay to a retreating intruder. The primary delay element, then, is the perimeter fence. The purpose of the fence is to keep the mildly curious person out, and to delay the retreating intruder.

Another delay mechanism which is simple, effective and can be used within the building itself is the installation of an electric lock on the front entrance to the lobby. The lock on this door would be normally open, and when actuated would lock. The door leading from the lobby area into the inner station would be normally locked and would release when actuated. If someone became unruly and threatening in the lobby area, the officer could effectively capture him by remotely locking the front door. It would also provide the officer a quick means of response if he saw an armed mob advancing on the front door. It might not prevent them from entering, but it would provide additional time for the officers to prepare their response.

6.4.3 Personnel Control

In order to implement an effective security system, it is essential that both authorized and unauthorized individuals be required to follow all personnel control procedures. Some salient personnel control guidelines have been identified and are outlined below.

PERSONNEL CONTROL GUIDELINES

Unauthorized

a. Public access to reception lobby only.

b. Citizen must be escorted at all times within station.

c. Outer areas should be fenced to keep public as far from building as is practicable. This includes the approach walkway to the reception lobby.

d. All areas surrounding building are to be used only by authorized individuals.

e. Public parking should be physically isolated from police vehicle and police private-vehicle parking.

f. Entrances and exits for prisoners should not pass through reception lobby.

Authorized

a. Personnel vehicles are to be parked in designated spaces.

b. Areas immediately surrounding the building must not he congested and allowed to impede police vehicle traffic.

c. All personnel and vehicles entering facility grounds must use proper identification procedures. If an officer forgot an ID transmitter, for example, he must park his private vehicle in the public parking area and gain access to the building though the public lobby.

d. All officers entering the inner building through the must be personally recognized by the officer on duty before the inner door is opened.

e. All officers must immediately report to the station captain, the theft or disappearance of any identification mechanism.

Detailed personnel control procedures must be generated, with regard to the specific operations and physical configuration of each individual facility. The above points are given only as guidelines in the prepagation of such procedures.

SECTION 7

SYSTEM RECOMMENDATION SUMMARY

7.1 GENERAL.

A fair number of security subsystems have been previously discussed, and recommendations have been made for each subsystem component of a total integrated security system. These elements have been selected to complement each other and enhance the performance of the entire system.

One of the major advantages in providing security for a police facility is that a 24-hour-resident response force is available. The prime objective, then, of a police facility security system is to provide the existent response force with various tools which will augment their senses, give the earliest possible warning, provide physical protection, provide intruder delay mechanisms to extend the time over which an effective response can be made, and to assist in intruder identification. In the selection of the subsystem elements, emphasis was placed on simplicity, reliability, flexibility, and low cost, consistent with the required function. It is the purpose of this section to summarize these various recommendations and provide approximate costs for each of the subelements.

7.2 TYPICAL STATION IMPLEMENTATION.

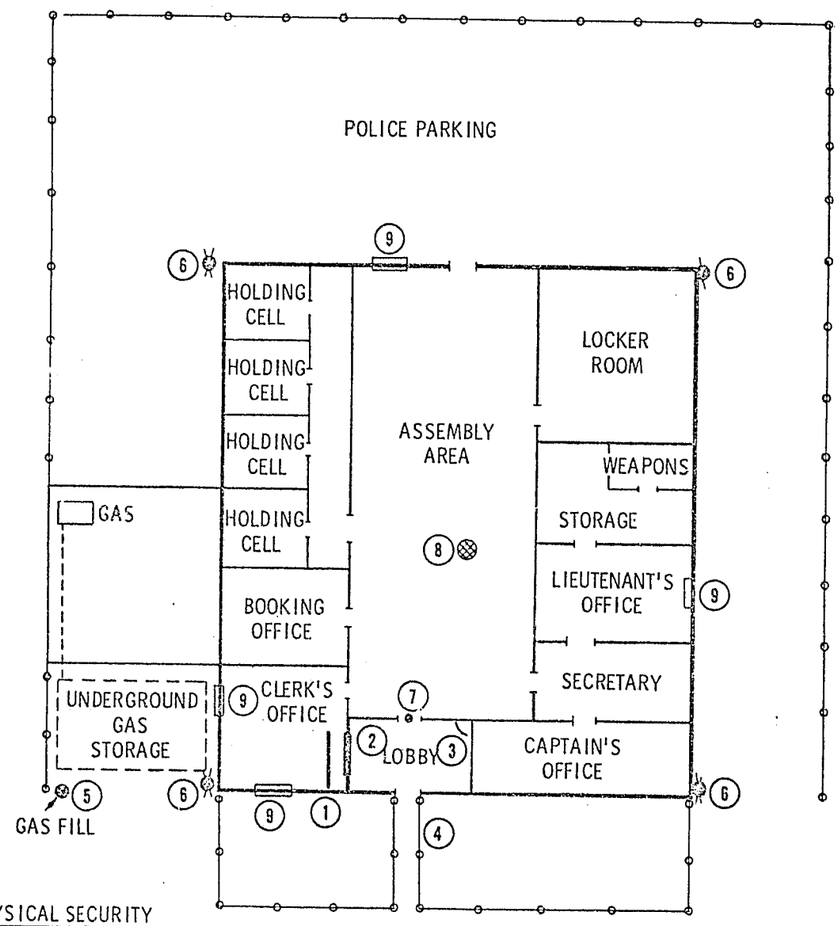
The best way in which the various recommendations can be summarized is to illustrate their use in a "typical" police-facility installation.

Each recommendation will be shown applied to this "typical" police facility, and its function will be described. For the sake of discussion the overall security system recommendations are broken down into four major subsystems. Physical Security and Deterrence, Intruder Detection, Communications, and direct assistance systems for the Response and Control Force.

7.2.1 Physical Security and Deterrence.

Physical security devices act as deterrents. The existence of fences, lights, barriers and an electronic detection system will keep all but the strongly motivated out of the facility.

Figure 7-1 illustrates a "typical" police facility to which various physical-security items have been applied. These physical devices should be the first consideration in implementing a security system. The figure illustrates a building surrounded by a fenced



PHYSICAL SECURITY

1. VISUAL BARRIER
2. BULLET PROOF GLASS (WITH AMPLIFIER) METAL PLATE UNDER COUNTER
3. CONVEX MIRROR
4. FENCED PUBLIC ACCESS
5. LOCK
6. LIGHTS
7. ELECTRIC LOCK
8. FINE MESH HEAVY SCREEN ON ALL VENTS
9. BULLET PROOF VISUAL ACCESS

Figure 7-I Physical Security Applications.

parking lot into which only authorized vehicles should be admitted. The fence should be of a chain link type, #2 mesh, #9 wire, 8 feet high, topped with three strands of barbed wire. The fence is the "first line of defense" in the security system. In order to negate bomb implantation, the public should be kept as far from the outside of the building as is practical. This philosophy should be carried through even in the public approach to the building. It can be seen in the illustration that the public has no direct access to any outside walls of the building. Usually this is not practical for the front of a building. In this case, as in all others, shrubbery and all clutter should be kept as far from the building as possible. These areas make excellent concealing places for bombs.

Most attacks take place at night to take advantage of the cover of darkness. Properly installed lights directed away from the facility serve a two-fold purpose - they act as a good deterrent, and they provide the officer the capability to readily survey the area.

If any gasoline is stored on the premises it must be stored underground, and the fill port should be secured with a padlock. Service personnel supplying gasoline should always be directed to the facility to have the lock unlatched for them. Careful key control is essential for all locks.

All entrances and exits into the authorized parking facility should be kept to a minimum, and preferably should have electrically actuated gate mechanisms. The details of implementing good gate control are given in Section 6.4.1.

The only windows in the facility should be strategically placed to allow the officers maximum visibility to the surrounding areas. These windows should be bullet-resistant (preferably to high-power rifles). All other windows should be structurally blocked.

All vents on the walls or roof should be covered with a fine-mesh heavy-gauge screen to preclude bomb placement. Unauthorized persons must be kept away from air intake vents.

The public should have free access only to a reception lobby at the front door. The lobby preferably should be rectangluar in shape with the business office at one end, as shown in Figure 7-1. No nooks or crevices should be present where bombs could be easily secreted. The clerk must have a full capability for visual surveillance of the lobby area, including the base of the reception counter. This can be accomplished through he use of convex mirrors. The clerk's reception desk should have a bullet-proof metal plate under the counter, with a transparent bullet-resistant material above the counter. A bilateral amplifier system should be installed so the clerk can easily hear the party on

the other side. If the bullet-resistant material is not continued to the ceiling, the gap between the top of the glass and the ceiling should be otherwise filled to preclude the throwing of bombs over it. A visual barrier should be placed approximately four feet behind the counter to preclude a potentially berserk person from opening fire on all persons within the business office. Only one person is to be seen by the public and he can quickly take refuge as required.

Electric locks should be installed on the door leading from the lobby into the inner station and on the front door. Both of these locks are controlled by the clerk. The lock on the door leading to the inner station should be a "normally locked" type which releases when it is actuated. The lock on the front door should be a "normally open" type which locks when actuated. The function of the inner door lock is obvious - it keeps all but authorized personnel out of the inner part of the station. The lock on the front door actually serves two purposes. If a person in the lobby threatens the clerk or the facility, the clerk has the capability to instantly capture him simply by actuating the front-door lock. The lock also provides an instant response if a threatening crowd moves toward the front door. The locked door may not stop the crowd but it will provide valuable delay time.

7.2.2 Intruder Detection.

A large variety of intruder detection systems are discussed in Section 6.2. The primary function of intrusion detection systems in application to police-department facilities is to give the monitoring personnel the earliest warning of unauthorized intrusions. These devices are "alert" 24-hours a day and will immediately report any activity.

No need was identified for any exotic detection systems. All of the recommended systems are simple and reliable and can be installed with relative ease. A summary tabulation of the recommended intruder detection systems versus their applications is given in Table 7-1. Detailed discussions of their operation are given in Section 6.2.

7.2.3 Communications.

In keeping with the general requirements of simplicity, flexibility, reliability, and ease of installation, an alarm communication system was selected which combines the functions of installation, line supervision, alarm transmission, display and alarm verification in a single system. The system uses existing power lines for transmission of alarm information. All that is required to install an alarm system is to interconnect the sensor device (such as a magnetic switch) to a Remote Alarm Transmission Device and, in turn, connect the device to the nearest wall outlet. The Monitor Display is

installed at the monitoring point simply by plugging it into an AC outlet. The alarm system installation is then complete. When an alarm occurs, the monitoring operator has the capability of selectively listening to the area in alarm. In this way, he can determine the nature of the activity taking place.

A complete discussion of this alarm transmission system is given in Section 6.3.3.

TABLE 7-1. SUMMARY OF DETECTION DEVICE APPLICATIONS

Protected Area	Sensor Device (in order of preference)
All entry portals into building	(1) Balanced magnetic switches (2) Properly concealed switch mats (3) Beam-breakers (IR CW)
Critical areas within building (weapon and record storage, communications, etc.)	(1) Balanced magnetic switch (2) Properly concealed switch mats (3) Beam-breakers
Roof	(1) Adapted continuous-line vibration sensor (2) Adapted tape switches
Outer perimeter	(1) Continuous-line vibration sensor (2) Taut wire (3) Beam-breakers
Gates	(1) IR modulated beam-breakers

7.2.4 Response and Control Force.

The task of controlling personnel, both authorized and unauthorized, lies with the Response and Control Force. This activity can be assisted by physical-security equipment to deter people from entering limited-access areas, and by intrusion-detection equipment so that the R&C force may be apprised of an intrusion the moment it takes place. Generally speaking, however, the R&C force has had to bear all of the burden of the discrimination of authorized from unauthorized intrusions -- be it a 24-hour guard post, or a strategically placed CCTV system, it is incumbent upon the R&C force to identify personnel.

A cost effective system has been devised to assist the R&C force in the identification of authorized versus unauthorized intrusions into the limited-access areas surrounding a police facility. Such a system is illustrated in Figure 6-5 as an "open gate" system.

Double infrared-modulated beam-breakers are installed at all normal openings into the limited-access area. The double beam-breakers allow the automatic determination of an exit from or entrance into the area. If an exit is being made, nothing need be done. If an entrance is detected, then a sign will flash which bears the word "Identification". (The sign can be eliminated if police personnel are adequately instructed on the use of the system.) The intruder then has a predetermined period of time to identify himself (of the order of 5 seconds) before an alarm is generated at the display console. If the intruder is an authorized person, he will identify himself (within the predetermined time period) by means of a changeable-code pocket transmitter. He simply presses the button on the transmitter, which sends its coded signal a few feet to a long-wire antenna which is placed around the building. The receipt of a valid coded signal negates an alarm response. The system provides an effective means of automatically separating authorized from unauthorized intrusions. The guard is alerted only if an unauthorized intrusion has taken place. The code on the transmitter and receiver can be easily changed on a random basis to preclude the use of a stolen transmitter by an unauthorized individual.

A full discussion of this technique (including "closed gate" systems) is given in Section 6.4.1.

A simple yet very effective mechanism can provide added assistance to the R&C force in capturing an intruder. This is done simply by providing the desk clerk the capability to remotely control the gates and doors into the facility. An example of this is the installation of an electric door lock on the lobby door. In the event someone charges into the lobby brandishing a weapon, or is belligerent, the clerk can capture him simply by pressing a button to lock the front door. The clerk then has ample time to take him into custody.

7.3 Cost Factors.

Throughout the formulation of an effective, integrated police-security system emphasis was placed on maximum performance for minimum equipment and installation costs. All of the recommended equipment and techniques are considered to be of a minimum cost with respect to the function required of them. In order to allow an individual department to estimate costs for a specific application, a table has been generated (Table 7-2) which gives cost estimates for each of the elements within the integrated security system.

In generating a cost estimate, one should first review his specific facility with respect to the recommendations given in this report. A list should be made of the number of each security element required for the specific application. The equipment costs can then be determined through the use of Table 7-2.

TABLE 7-2. SECURITY SYSTEM ELEMENT COSTS

Item	Approximate Cost	Remarks
Physical Security Items		
Chain link fence (#2 mesh, #9 wire, 8 ft high with 3 strands barbed wire and top rail)	$4/ft	Installed
Bullet-resistant glass (1-1/2 & 2 in.)	$16-$24/ft^2	High-power small arms: 1-1/2 in. High-power rifles: 2 in. (in approx. 200 ft^2 quantities)
Convex mirrors (13 to 36 in. diameter)	$14 to $70	
Electric locks	$40	
Five-button combination mechanical door locks	$40	
Remotely controlled gates	$1400	Radio controlled for gates up to 45 ft wide
Intrusion Detection Items		
Simple magnetic switches	$2	
Balanced magnetic switches	$45	Weather resistant, tamper switch & anti-flash welding contacts
Switch mat	$21	18 in x 36 in mat (indoor only)
IR modulated beam-breaker	$300-$500	
Continuous-line vibration sensor for perimeter	$0.50/ft	+ $350 per sector for signal processor*
Adapted continuous-line vibration sensor for roof	$1.25/ft^2	+ $350 for signal processor*
Taut-wire fence sensor	$1/ft	+ $140 per sector for alarm display
Photoelectric beam-breaker	$60	
Alarm Transmission System		
Display unit	$250*	
Receiver & transmitter modules/pair	$200*	
Automated Identification System		
Receiver and logic	$500*	
Pocket identification transmitters	$40	

* System not developed - costs are engineering estimates for production units

The largest variable cost factor will be the installation cost. Because of the variety of physical configurations of police facilities and the variation of labor rates across the country, it is impractical to quote installation costs as dollar figures. In general, installation costs can vary anywhere from 50 percent to 500 percent of the material costs. It should be noted, however, that all of the equipment recommended is relatively simple and, this being so, installation costs should be minimal.

As a first-order approximation, installation costs could be taken as 75 percent of material costs. This will provide a rough order of magnitude of the total cost for a secured police facility.

SECTION 8

SECURITY PLANNING FOR NEW BUILDINGS

The preceding sections have dealt primarily with cost-effective security measures which may be applied to existing police facilities. In the event that one is currently planning a new facility, however, a variety of considerations must be entertained in order to ensure the construction of a secure facility. The following sections discuss these security considerations in terms of the station's function, configuration, construction and procedures.

8.1 STATION FUNCTIONS AND FLOW.

A police facility can be defined as comprising three major functional elements. Almost every facility must first serve the public, provide prisoner processing and detention facilities, and provide space for all of the staff functions. This is basically illustrated in Figure 8-1.

Most police facilities are divided into three departments or elements, which are the services group, field operations, and investigation. This is shown diagrammatically in Figure 8-2. As the three basic bureaus or departments are expanded, they can be illustrated by the organizational chart shown in Figure 8-3. In this particular chart, the operations bureau covers not only the field patrol, but the investigative section as well. The services bureau is primarily interested in the functions pertaining to records and identification, communications, and the jail. The administration bureau includes the upper administrative group, and such additional activities as planning and research, personnel and training, inspections, public information, etc. Almost every department follows this basic pattern, with some few exceptions. In the smaller police department of course, some of these functions are totally missing, and others must double or triple their areas of responsibility.

One of the relatively new police departmental organizational charts is shown in Figure 8-4. This modified mode has departments still divided into three basic bureaus or sections, but with some of the functions related to the administrative assistant and the police chief rather than assigned to a basic bureau. The modified model seems to be one of the most popular at the present time and seems to be especially attractive to the smaller or medium size department.

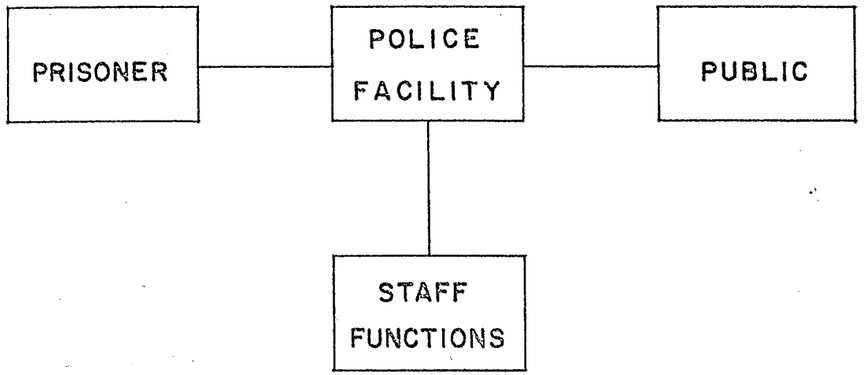


Figure 8-1 Three Major Elements of Facility Functions

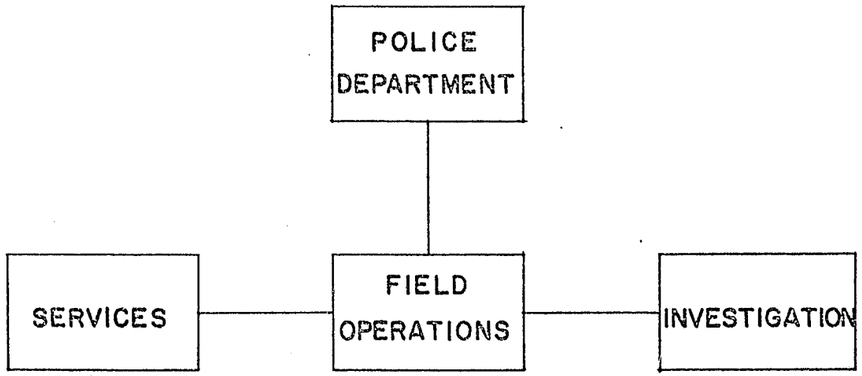


Figure 8-2 Three Major Elements of Department Functions

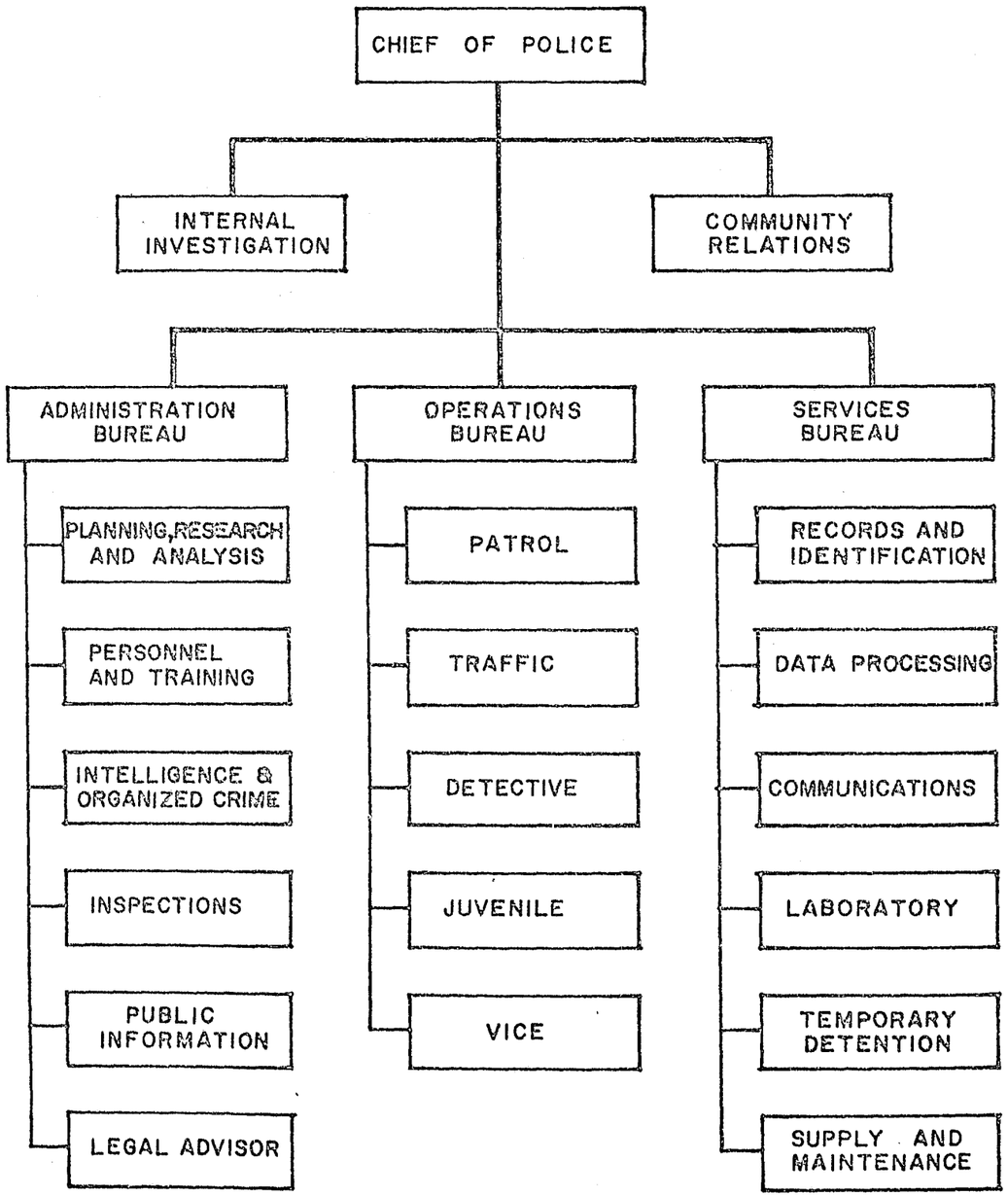


Figure 8-3 Typical Organizational Chart of a Well Organized Municipal Police Department

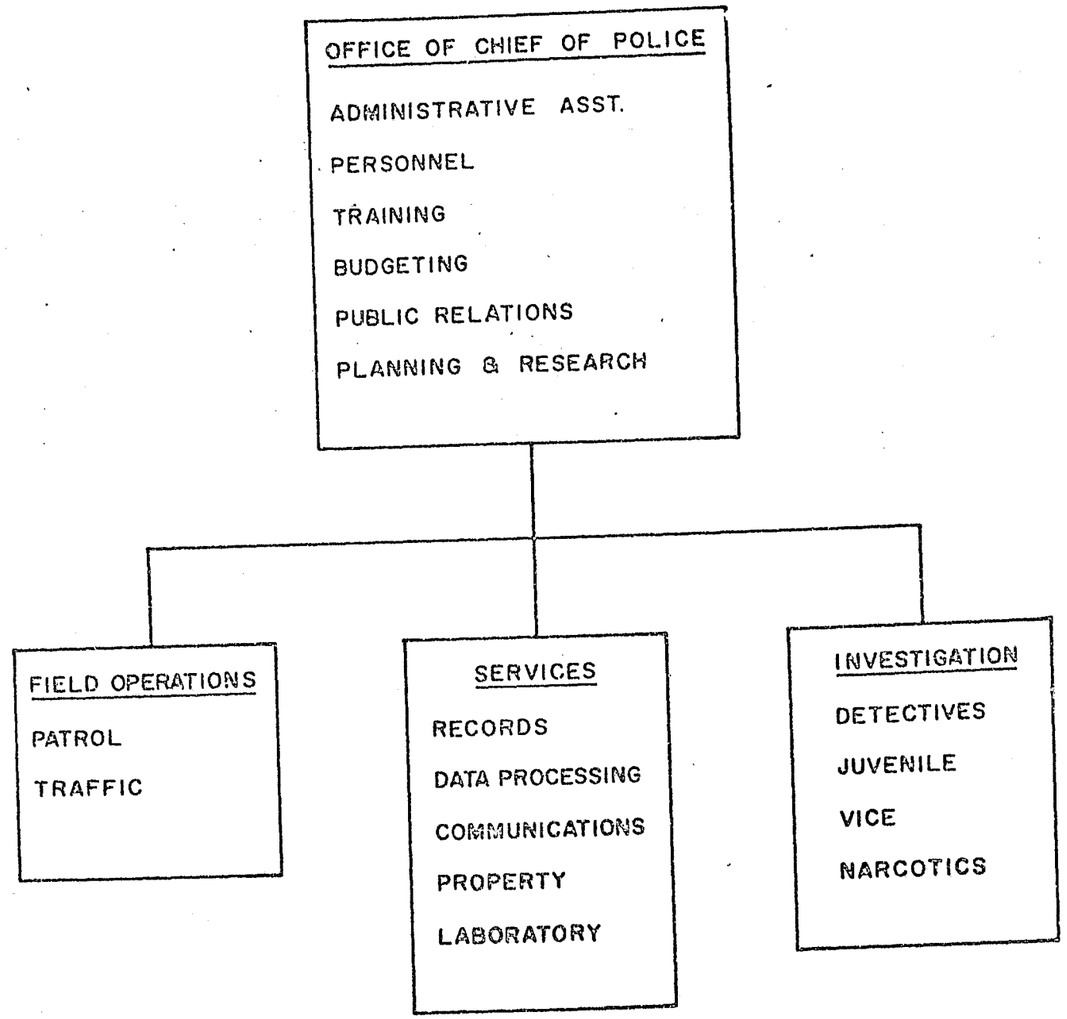


Figure 8-4 Modified Organization Model

Figure 8-5 is a diagram of a "Team Policing Model". This concept was first described by the late August Volmer of Berkeley, California, who wrote about the future role of the police officer as a "generalist". Several cities are experimenting with the team concept, but the effort is so new that an objective analysis and evaluation has not been possible. In the team concept, the entire staff is not divided into the three basic bureaus, but is divided into team groups, as shown on Figure 8-5. Each team would contain a specialist, with teams overlapping to provide continuity on any major crime.

Because this is an unproven concept, any new facility being constructed should not be planned specifically around the team concept, on the basis that if the team concept proves unsuccessful the facility should be usuable for a more standard departmental organization structure. The modified model as described in Figure 8-4 could be the basis for a "team" concept, yet still be related to the basic three-bureau department structure.

Figure 8-6 traces the processing of a prisoner, indicated by the dotted line, from an entrance sally-port through holding, booking, mugging and printing, and then either to the drunk tank or to jail or the detention portion of the building. The public's only contact in this area would be to visit a prisoner, or for an attorney to visit his prisoner client. Staff would enter the jail or the security area only for limited reasons. The prisoner and the public would always remain totally separated.

Figure 8-7 shows some of the spaces related to a detective bureau. In a larger facility, a captain might head this bureau and the department would include a number of lieutenants. Additional areas used by this group are interrogation rooms, a recording monitoring room, supplies, a detective locker room and toilet room, and a conference room. Every function of a police department can be analyzed in a similar manner.

Figure 8-8 shows the communication command center for a department of size similar to that of the model we are illustrating in this report. In the command center itself, it would contain the communication console, but would have its own internal functions such as coffee room, dispatcher's locker room, toilet room, communications director's office, and the phone and communication equipment spaces. The watch commander might not be directly adjacent to the communication command center, but through the various means of communication would remain closely related to this function. These plates have been included to illustrate some of the analysis that should become a part of the evaluation of the structure of any police department by the architect before he commences the actual plan or design process.

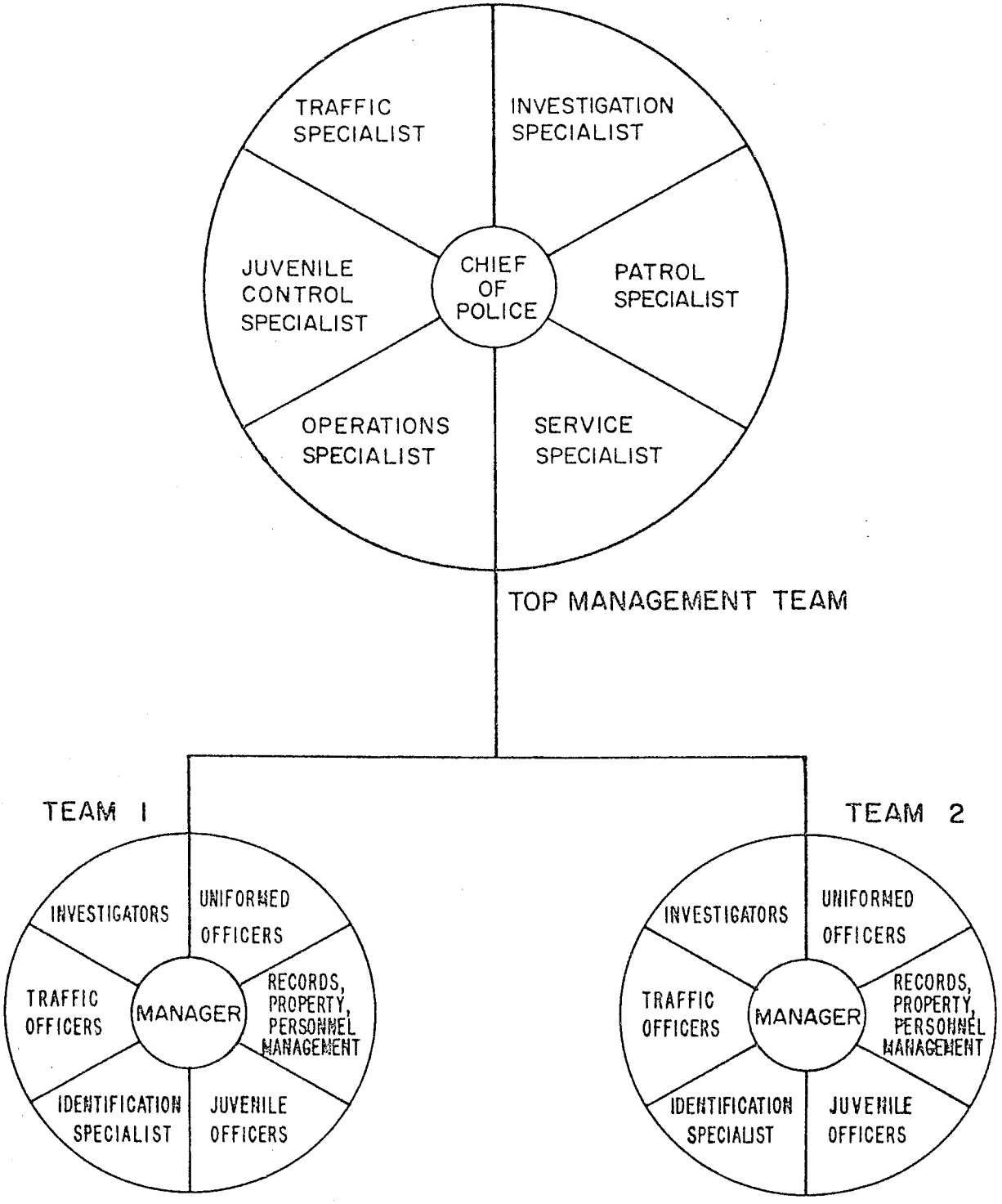
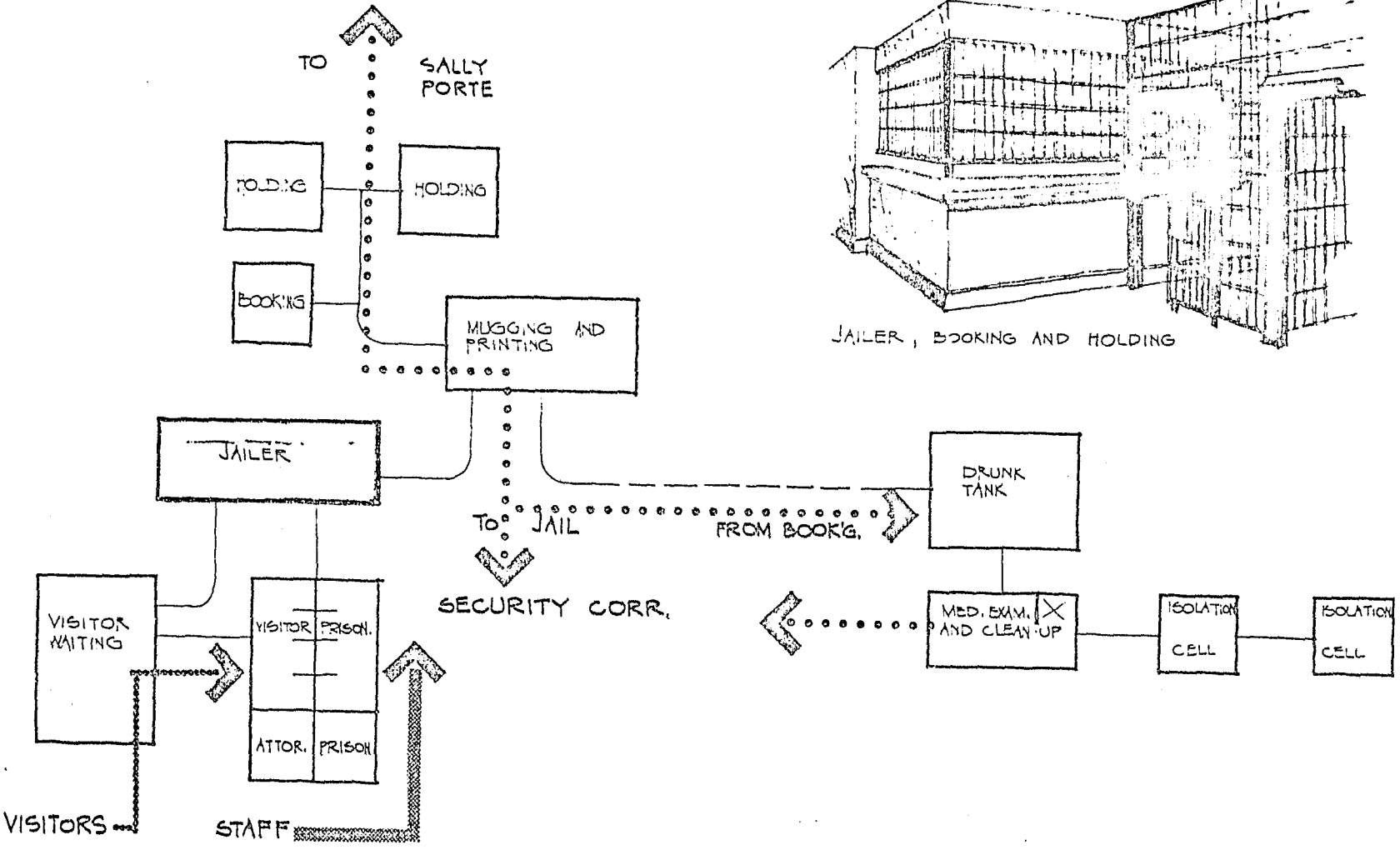


Figure 8-5 Team Policing Model



JAILER, BOOKING AND HOLDING

Figure 8-6 Prisoner Processing

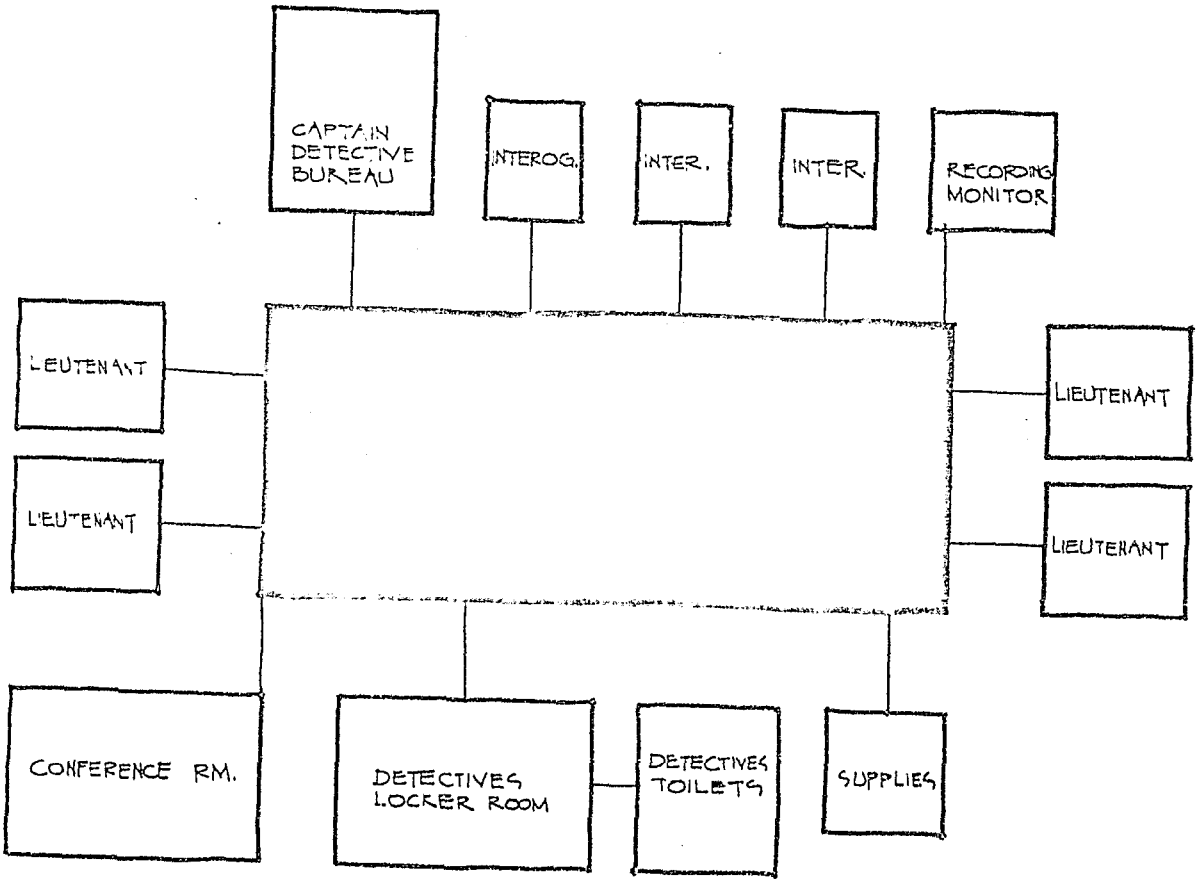


Figure 8-7 Detective Bureau

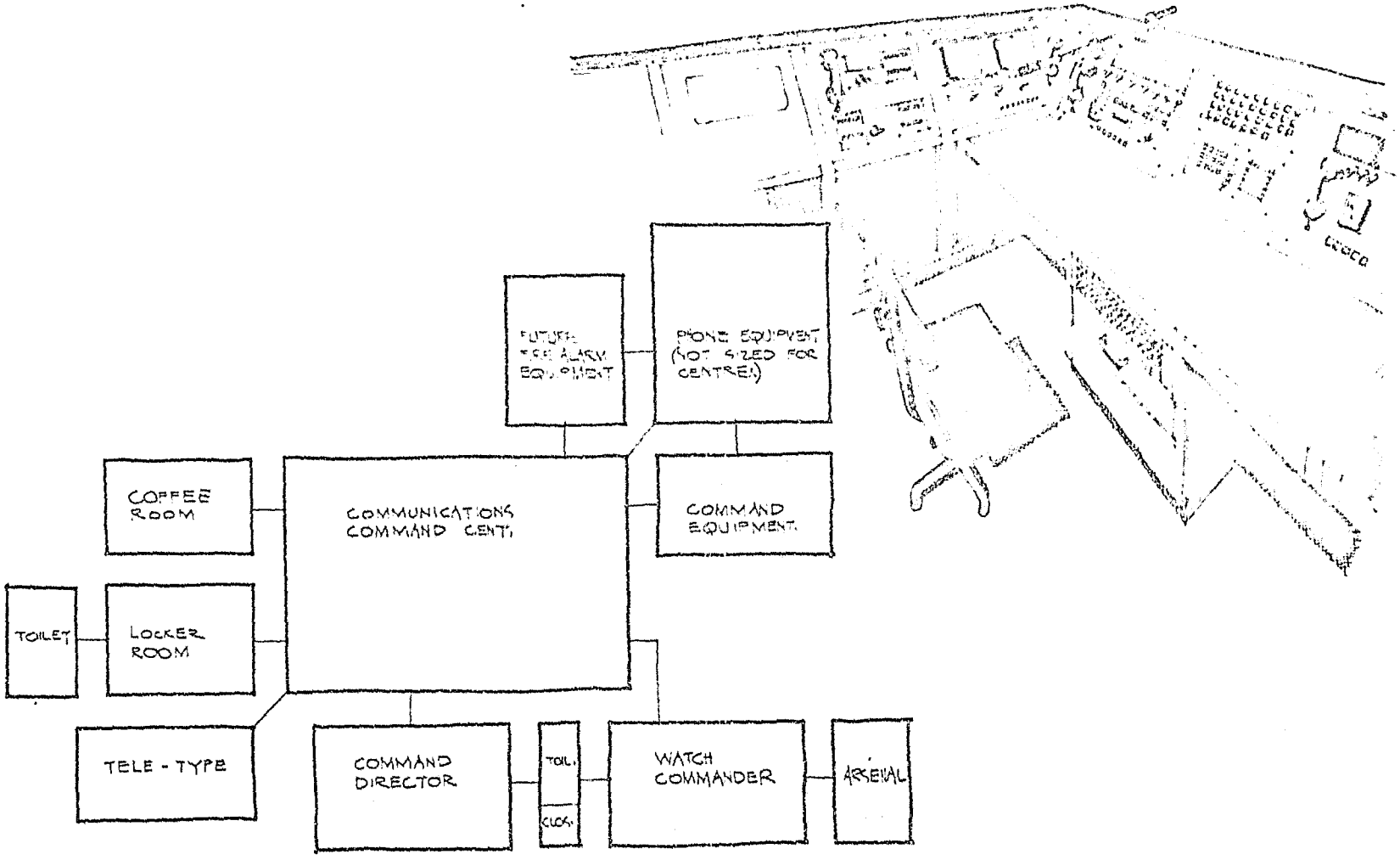


Figure 8-8 Communications Command Center

8.2 TYPICAL STATION LAYOUT.

Figures 8-9 and 8-10 illustrate the various basic parts of a model police facility and their proper relationship to each other. This facility is a basement-and-one-story building primarily designed to illustrate more clearly these relationships. When the site is limited, then, of course, the building might be a basement-and-two-story in place of the single story as shown in the model; however, the function and the circulation would remain the same, and could develop the same control and efficiency as described in our model.

8.2 1 Typical Facility - First Floor.

One of the basic concepts of the proper planning of a police facility is to isolate as much as possible the internal circulation required by the public, the staff, and the prisoner. In today's facility aimed at developing maximum security and control not only for the prisoner, but in relationship to the public, some new planning techniques have been developed. For example, the public enters the building into the lobby area through a single public entrance (Figure 8-9). The lobby is separated from the balance of the building by doors remotely controlled by electric locks. The lobby contains the complaint counter, which is the first point of contact when seeking service from any one of the departments. This area also contains a suitable waiting alcove.

The public is not permitted to penetrate further into the building unless by permission. This means that all of the public circulation within the main body of the building itself is by control and with some degree of supervision. If a person is suspected of carrying contraband, then, of course, this person is further screened before being given permission to circulate further within the building.

The area marked Duty Sergeant or Watch Commander is shown near the record room area only because a person occupying this position might need to cover the lobby on the graveyard shift. In this typical facility, the communication command center has been remotely located in the basement of the area and is not immediately adjacent to the lobby. In smaller facilities, the communication dispatcher is required to service the lobby on the late shifts.

The investigative bureau shown on the left-hand side of the ground floor has the main group of detectives located in the large room known as the bull-pen. Interrogation rooms and a polygraph room are immediately available from this larger space. Also located nearby is a separate smaller space for one or two detectives servicing narcotics and vice. An additional portion of the detective bureau primarily concerned with juveniles has been located immediately adjacent to the lobby. In smaller facilities the juvenile activity does

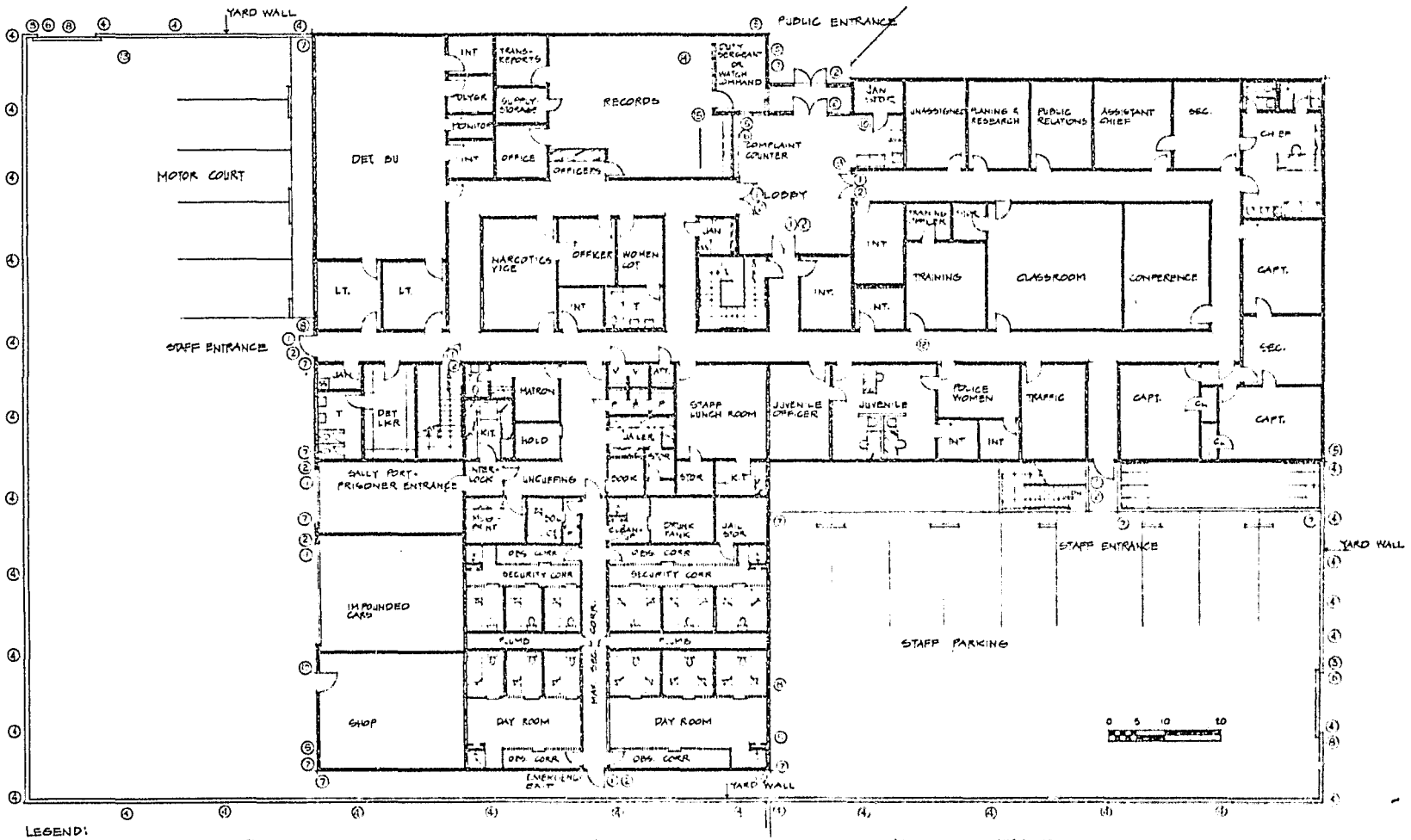
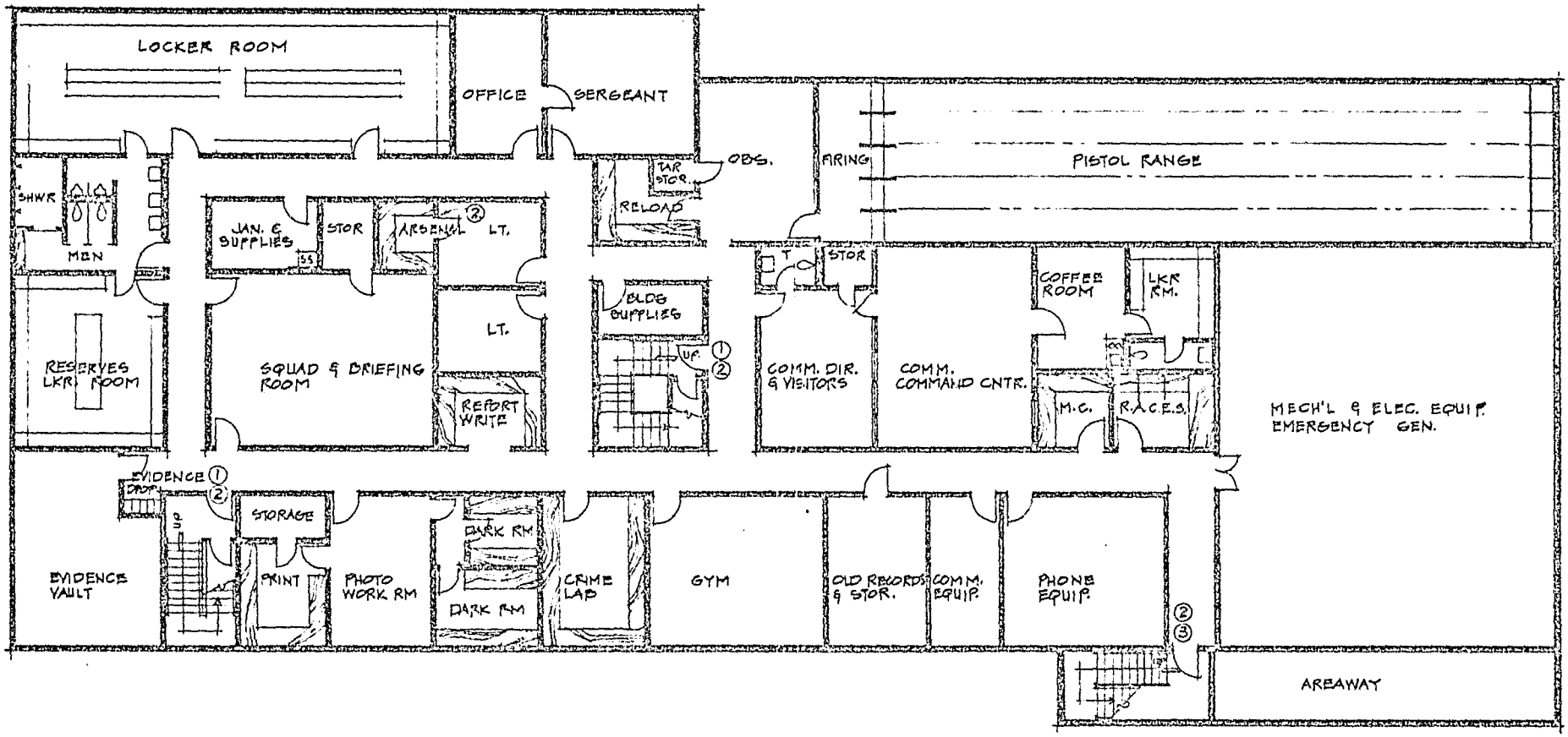


Figure 8-9 Ground Floor Plan of Model Station



LEGEND:

① ELECTRIC LOCK

② DOOR SWITCH

③ COMBINATION LOCK

0 5 10 20

Figure 8-10 Basement Floor Plan of Model Station.

not require a separate office grouping, but in a department of this size two or three officers along with a policewoman are assigned to this special activity. Access is near the lobby for convenience, and to separate this group from the balance of the adult detective or investigative activity. A classroom located almost directly across from the juvenile bureau can be used as a hearing room or for group conferences with juveniles and their parents.

The jail portion of the project, which includes prisoner processing and visiting is located on the ground floor of the project to simplify and minimize prisoner handling at or within the building. The jail is located near the investigative or detective bureau as this group is the part of the police department that has the greatest contact with the prisoner. The prisoner enters the building through a sally-port, with the entrance doors and the inner door interlocked for maximum security. The holding cell near the entrance door is separated from the booking activity, which simplifies the removal of contraband and other personal effects from the prisoner. The jailer's office is used for the booking operation and the storage of personal effects. In the uncuffing area is also the mugging and printing room all conveniently located for simple and safe prisoner processing. A matron's room is located in this area, as many facilities do not have sufficient staff to maintain a matron available on a twenty-four-hour basis. The prisoner visiting and attorney's visiting are conveniently located to allow maximum security for the prisoner, yet avoid bringing the visitor or the attorney into the security or processing areas.

The jail or the detention area has been divided into four main cell-block sections, along with a solitary cell and a drunk tank. Each cell block can be used for a different "type" of prisoner, as required for proper and legal segregation. Any cell can be used for either male or female, depending upon the occupant load. The day room has been suggested for two of the cell blocks, primarily for the purpose of serving as a temporary holding area for a large group that might be required to be detained in the jail area for a short period. This would be true during any kind of civil disorder, major labor unrest, high school gang fights, etc. The jail is not necessarily intended for sentenced prisoners; however, the cell block with the day room is designed to be similar to a sentenced-prisoner accommodation in a larger detention facility.

The record room area located adjacent to the lobby serves as the facility work pool, main prisoner bookings and record keeping, and services the public at the complaint counter. A separate officer's counter is located as a part of the record room activity and is used strictly for servicing staff. The right-hand wing of the building contains the main administrative group consisting of the police chief and his assistant and their

secretary, the three division or bureau captains, and a single secretary serving this group, conference room, and the training officer and classroom. In addition, several other offices used as planning and research, public relations and unassigned office are located as part of this activity.

One of the most accepted arrangements for upper-echelon administrative staff is to accommodate the chief, his assistant, and the captain, in one area of the building. In some of the earlier facilities, the captains were located near their particular departments or bureaus as being more convenient, or closer to their staff. This particular closeness tends to dilute their effectiveness as upper-level administrators, and often the department head performs services which should have been assigned to lower-echelon people.

The plan has been oriented to include a separate police-car parking lot, shown at the left-hand side of the plan, which would contain sufficient space for police vehicles, some covered vehicles, storage carports, the found-property storage room, and similar activities. There is a separate staff entrance from the police motor court, and a separate prisoner entrance, as shown.

A staff parking lot is located near the administrative wing of the building, with its separate staff entrance. An exterior stairway leads to the basement area for convenience of staff entering the building with a primary interest in the basement-level activities. A stairway near the staff entrance adjacent to the police motor court also leads directly into the staff basement area.

8.2.2 Typical Facility - Basement.

The basement area of the facility (Figure 8-10) accommodates a number of departmental activities, but none directly related to public contact. The only public entrance of the basement would be for the purpose of visiting either the pistol range or the communication command center.

The patrol, or uniform, division works almost exclusively from the basement area. Their locker room, toilet room, squad room, briefing room and report-writing area are all located in the basement. In addition, there is a locker room for the police reserves, evidence vault, photographic workroom and darkrooms, a small crime lab, a pistol training range, a physical training or exercise room, the communication command center, and the mechanical/electrical telephone ond communication equipment rooms.

The basement area ha. been designed with sufficient space and of such configuration that it would be ideally suited for a federal civil defense emergency operating center complex. The space in the basement listed as MC near the command center and ranges

is intended to be used strictly for civil defense needs. One is the message center and the other is for the amateur radio transmitters planned as a backup for the city's police radio systems.

The communication command center is a self-contained unit with its own coffee room, locker room and toilet room, and the communication director's space. The employees could remain in this area during their shift, which affords maximum efficiency and security. The only person entering the communication director's office would be a visitor interested in viewing the command center function.

The pistol training range is a standard 75-yard, 5-lane range which is the size generally recommended for every police facility.

This typical facility, as now projected by our basement and ground-level plan, could easily serve a city in the 50,0000 population range. The average staff for a city of this size would be about 75 to 80 sworn personnel.

8.3 STATION CONSTRUCTION.

8.3.1 General.

Every public building should reflect a design atmosphere of restrained dignity, permanence and security. This should be especially important for every police facility, as the police facility does as much as any other activity in the city, to create a public image for the city and its governmental staff.

A superior architectural design effect can be achieved at the same time, to develop an aspect of security for the building and its occupants, without an obvious effort to create a "fortress". The architect should thoroughly understand all phases of the elements that improve building security and safety, and with these tools then use his ingenuity to create a successful design.

In the construction of any building, whether it be for public or private use, many factors contribute to the programming of the building constructed for maximum security. One of the important elements often overlooked by architects and owners alike is the basic shape of the building itself. In addition, not only the shape but the texture of the vertical surfaces becomes very important. The Federal government has found, on the basis of their many studies of Federal buildings, that vertical building surfaces with many ledges, recesses, screens, deep window reveals, etc., made it easy for the saboteur to place a bomb.

Figure 8-11 illustrates several basic building shapes that represent almost all building possibilities. It should be obvious that as the building shape includes more recesses, courtyards, and changes in wall surfaces, it becomes more vulnerable for sabotage by creating areas hard to observe or supervise.

One of the most basic shapes for any building would be the square or rectangle. This building is one that would have four outside corners, without any inside corners, or courts, or yards. This shape is the easiest from which to observe outside wall areas. It might also be described as potentially the safest, with the probability of being the most economical to construct.

The other building shapes shown on our diagram all present some additional security problems. The public access to some of the spaces created by wings of the building could affect the level of building security. For example, an L-shape building where the L or inner court is the police parking lot surrounded by a wall and not normally for public use or access could still be the quivalent of the rectangular building. The basic shape of the building, of course, must reflect the size and shape of the lot and the site development required. For example, a police facility often requires a separate parking lot for police cars only. an off-street parking area or lot for staff, and an additional parking area for public use. Most buildings requiring off-street parking are concerned only with automobiles and not with the degree or level of segregation as described above.

It is recommended that landscaping be kept back or away from the vertical walls of public buildings, and this space paved with concrete or covered with gravel, which would permanently separate building from landscaping. Any object placed near the building would then be easily seen by staff and would be easy for an exterior closed-circuit television camera to view.

Figure 8-12 shows basically that a police facility and jail are usually related to a police car parking lot surrounded by a wall or a combination of a service building and wall. This police parking lot is for police cars only, including the delivery of prisoners.

The service building is very often a covered-carport-type storage building that can house some of the bulk storage and activity not directly related to the police departmental function, and that could be constructed at a lower price. Some of the activities often placed in the service building are such items as impounded-car storage, communication repair shop and service area, found-property storage room, large-evidence storage room, and parking meter repair shop.

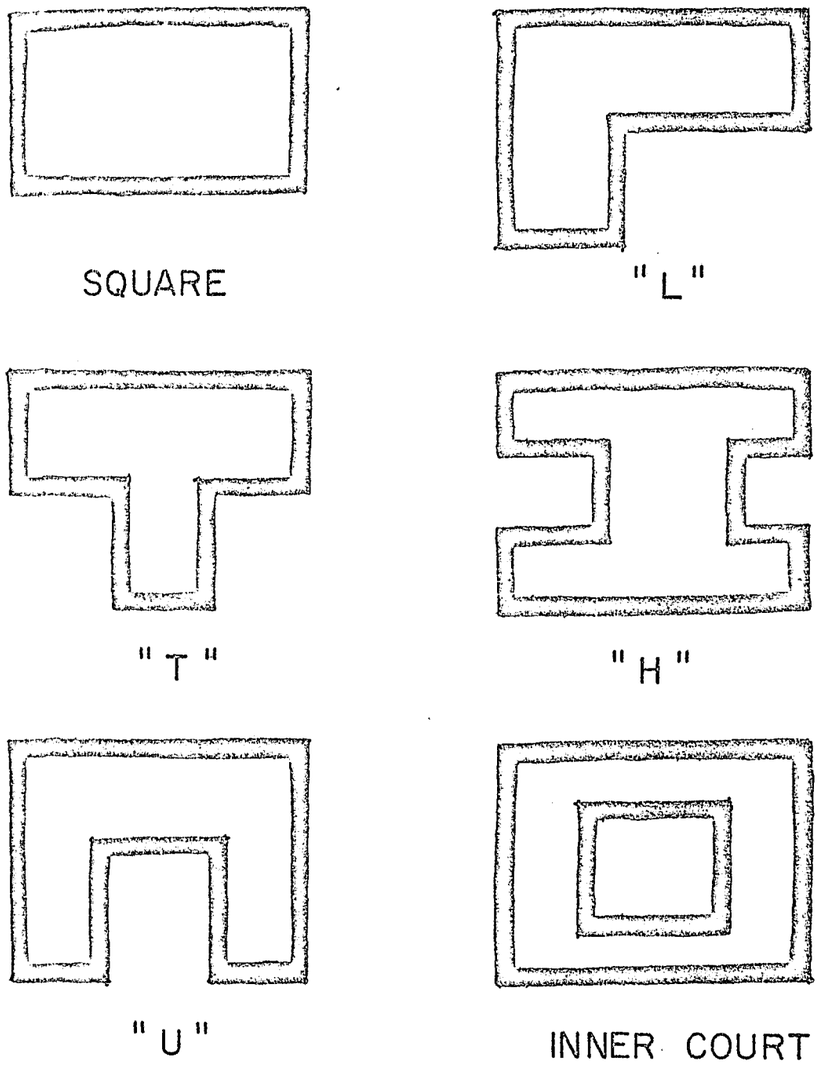


Figure 8-11 Basic Building Shapes

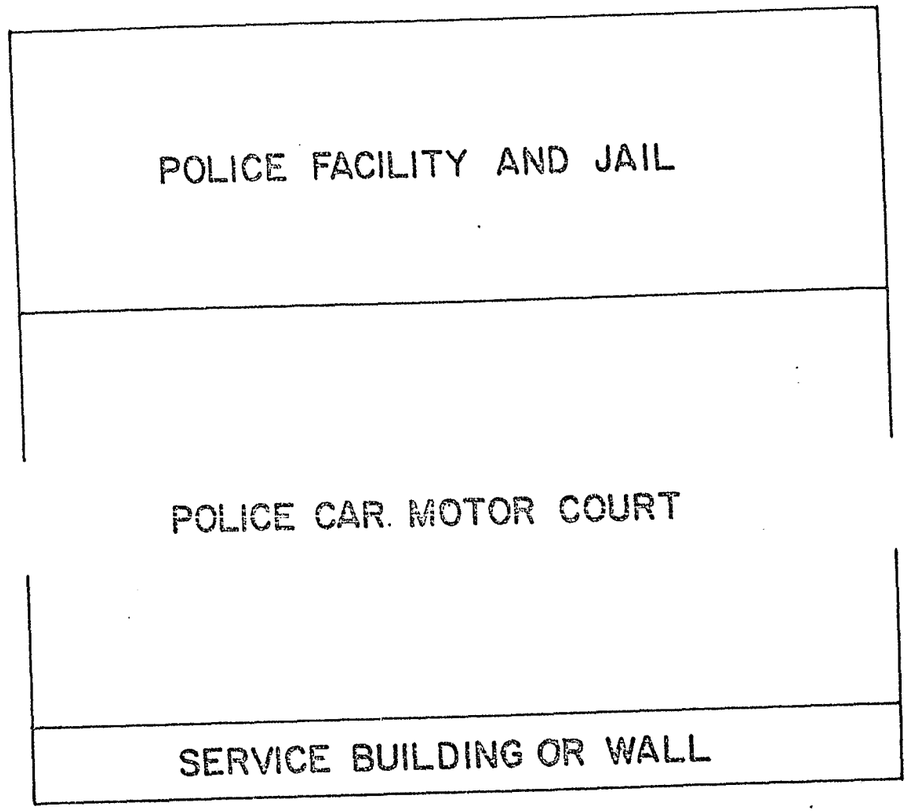


Figure 8-12 Layout of General Police Facility

8.3.2 Construction.

The basic recommended construction material or system for any police facility would be what is known as Code Type I or Code Type III incombustible. Code Type I is reinforced-concrete walls, with either reinforced-concrete floor slab or combination of steep structural system and concrete. The minimum fire rating for structural portions of the building would be two hours. Code Type III is masonry, which would be concrete block, brick, or a combination of block and brick. The interior structure and basic wall systems would be one hour.

In almost every state, the jail or detention portion of the building is required to be Type I, with all of the construction and materials used in that area to be incombustible. Most codes require an occupancy separation between the jail and the administrative portion of the building, varying between 2- and 4-hour wall construction In some states, the administrative portion of the building can be Code Type IV or combustible construction with a 1-hour minimum fire rating. The jail or detention areas would be separated by the 3- or 4-hour fire wall described above.

The exterior walls of the building should be reinforced, as for the systems used to resist horizontal seismic forces or wind loads. This reinforcing will resist blasts; the amount of resistance will depend upon the reinforcing and, of course the size of the bomb. None of the codes allow any protection factor against blasts if the wall is not reinforced. It is further recommended that wherever possible the roof slab, except on multistory buildings, be constructed of reinforced concrete The concrete provides more blast resistance at this level than almost any other structural system.

The exterior window openings should be minimized and placed at a level that would prevent an occupant from becoming a target. These glass or window openings should be glazed with a material that would at least resist rocks and bottles. Some materials are available that offer additional protection against small-arms fire.

The mechanical and electrical systems of the building should be designed for maximum security and protection, with a special effort to prevent easy vandalism. If the exterior walls of the buildings are solid and without any openings, then additional smoke venting devices should be installed at a number of strategic portions of the building that would allow venting in the event of a major fire. This requirement should be carefully reviewed with the local fire marshall to secure his recommendations. The use of extensive wood wall areas, millwork items and other combustible materials on the interior of the building should be avoided wherever possible. The building construction should be incombustible,

with paint and acoustical ceiling materials installed in accordance with standards of the fire marshal's office and state code recommendations

The staff areas should be separated from the public lobby by nonbreakable and bullet-proof glass at the complaint counters and by visual barriers behind the counters. The elimination of conflict between the public, police department staff and the prisoner by properly isolated and controlled corridors can do much to improve the security of the building and staff. Some of the major accidents that have occurred within such buildings occurred because prisoners had to be transferred from one portion of the building to another through a public corridor.

A properly planned and engineered building containing recommended basic improvements for security and safety can often be constructed without any increase in cost. The experienced architect with the cooperation of his client could and should do much to improve security and safety of these facilities with knowledge and effort rather than just an increase in construction cost.

Figure 8-13 is an illustration of a proposed new police facility for the City of Mountain View, California. The facility is restrained, has dignity, would create the apperance of permanence and security, yet the design elements have been handled in such a way as not to make obvious a number of very important recommended safety features. For example, there are no windows on the first-floor area exposed to the public. The main entrance is of glass, but limited in area. This limited glass area can be economically installed as bulletproof glass to achieve outward vision, yet maintain true security The second and third floors do contain windows, but the windows on either side of the building have been protected by bulletproof steel or fiberglass louvers. All of the surfaces within reach are smooth, without any projections for bomb placement. All landscaping has been eliminated from the vicinity of the building, substituting a paved plaza and walkway area.

8.4 VULNERABILITIES AND DETERRENCE.

The vulnerabilities of new police facilities and the deterrents which can be used advantageously in countering them are discussed in the following paragraphs. Figures 8-9 and 8-10 are used as references for the following text.

8.4.1 Basement.

Because the basement of the building is below ground level, and because there are only two entrances to this area, the basement is vulnerable to attack only in terms of scenario 5.3.2 (Bomb Placed Inside Buidling in Vulnerable Area), scenario 5.3.6 (Area Entered and Police Personnel Attacked) and scenario 5.3.6 (Incapaciting Gas Injected into Air Inlet).

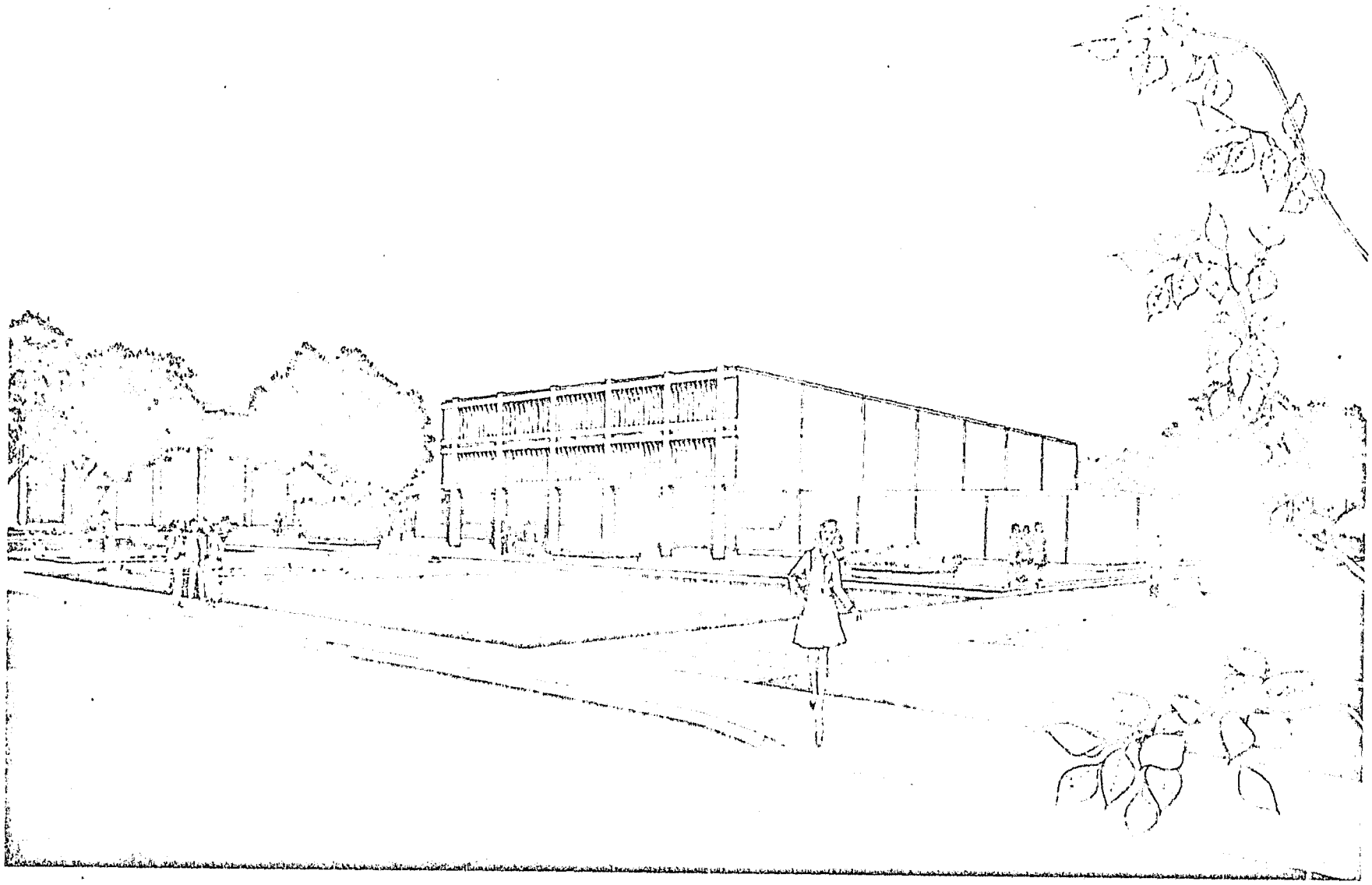


Figure 8-13 Mountain View Police Facility

The first two scenarios require that the attacker gain access to the basement. To preclude this possibility, the four doors, two for each stairwell, should have electric locks and door switches. The alarm information from the switches would be transmitted to the alarm status monitoring console via the power-line alarm transmission system. A less vulnerable plan would be to have only one set of stairs leading into the basement. However, traffic and procedures may require the two sets of stairs.

The third scenario (Incapacitating Gas Injected Into Air Inlet) does not require that the attacker gain access to the basement, but only that he gain access to the air inlet. The best countermeasure to this type of attack is to use a closed-loop air conditioning system. If this is not feasible, then steps must be taken to deny an attacker access to the air inlet port. This is best handled through the use of physical barriers.

No unescorted visitors should be allowed in the basement or the weapon storage area and the evidence vault should be equipped with a magnetic door switch.

8.4.2 First Floor.

The first floor is vulnerable to attack via all scenarios. The vulnerabilities and applicable countermeasures will be discussed for each previously identified scenario.

a. Bomb Placed Outside of Building.

To preclude this type of attack (in addition to good architectual design to eliminate convenient hiding places), it is necessary to detect unauthorized persons in the station area surrounding the building. To accomplish this, the following countermeasures should be taken:

(1) Beam-breakers across entry gaps into the parking area.
(2) Fences with a perimeter detection system around the station area.
(3) Bullet-proof glass -- enough locations to enable surveillance of all outside areas.
(4) Remotely controlled vehicle gates.
(5) Sufficient lighting so that identification can be accomplished at night.
(6) A system for automatically identifying authorized police personnel.

b. Bomb Placed Inside Building in Vulnerable Area.

The easiest place to leave an explosive charge is in the lobby. To prevent someone from leaving an explosive charge in the lobby station personnel should be alerted whenever anyone enters the station. Therefore, magnetic switches should be placed on the entry doors. There are two doors into the lobby. Both should be equipped with magnetic switches

so that station personnel know where civilians are located. The lobby should be designed so that no areas exist which cannot be surveyed by station personnel from the complaint counter. The lobby as shown in Figure 8-10 contains no alcoves where a bomb could be concealed. There is a convex mirror so that the area near the stairwell can be seen. Station personnel should be suspicious of any suitcases, handbags, parcels, etc. that are left in the station for any reason whatsoever.

The general public should not be permitted into the remainder of the station, and those that have business which requires that they be in other parts of the building should be escorted at all times. To deny the general public access to the remainder of the station, each door between the lobby and the other parts of the building should be equipped with an electric lock, as should the four external doors, except the door into the shop leading into the station. The shop door should be provided with a lock so that unauthorized persons are denied access to this area.

The vehicle doors into the sallyport and into the impounded-car area should be remotely controlled.

In order to minimize the effect of a bomb thrown into the lobby, a metal plate should reinforce the area under the complaint counter, and the area above the counter should be of bullet-proof glass. A baffle and an audio amplifier are required. A visual barrier should be placed behind the complaint counter separating the counter from the rest of the business office.

c. Bomb Placed on Roof.

The problem here is to detect that an explosive charge has been placed on the roof of the building. The previously recommended continuous-line vibration sensor will detect any activity on the roof.

d. Bomb Placed in Gasoline Storage Tank.

This vulnerability can be negated by having a lock on the gas fillter port.

e. Personnel Shot Through Windows.

The model building does not have any windows on the ground floor, which directly negates this scenario.

f. Building Entered and Officers Shot.

The security measures required to negate this vulnerability have already been itemized under the vulnerabilty to bombing attacks. In summary, the countermeasures are to prevent civilians from entering the building, except in the lobby, and to further protect police personnel from gun shots through the use of a metal plate and bullet-proof glass.

g. Bomb Placed In or Under Vehicles in the Parking Lot.

The first defensive measure is to prevent ready access to the vehicles by fencing the entire parking area. This, in conjunction with a perimeter system, will deter most attackers and detect those which are not deterred. The use of positive authorized personnel control procedures, lights, and bullet-proof windows, will allow identification of all persons entering the parking areas.

h. Incapacitating Gas Injected Into Air Intake.

The countermeasures to this type of attack is to place the air intake so that it is inaccessible as possible and also use subsystems described previously to detect unauthorized individuals in the station area.

i. Personnel Shot as They Move Between Vehicles and Building.

The only way to negate this vulnerability is to not expose personnel to such an attack. This can be accomplished by covering the parking area, or by providing a parking area in the building.

8.4.3 Display.

The outputs of all sensors will be channeled via the power-line alarm transmission system to a display console. This system is described in Section 6.3.3.

8.5 SECURITY PROCEDURES.

The security procedures discussed in this section are those procedures which should be employed with the security features discussed in Section 8.4. This combination of physical security features, equipment and procedures will result in a viable security posture.

a. As mentioned previously, all nonpolice personnel in areas other than the lobby should be escorted.

b. When the alarm system indicates that someone has entered the lobby, the complaint counter should be manned if there is no police personnel already there. In the process of conducting normal business, the officer should be sure that nothing that could contain a bomb is left in the lobby. The convex mirror has been provided to aid in this determination. Also, the officers should ensure that no unauthorized individuals in the lobby gain access to other parts of the building.

c. When a perimeter alarm has been registered, a visual inspection of the station area should be made, using the bullet-proof windows provided for this purpose.

d. When the roof alarm system indicates that an object has been placed on the roof, the building should be evacuated and the bomb squad called in to investigate the object and to deactivate it if it is a bomb.

APPENDIX A

QUESTIONNAIRE

QUESTIONNAIRE
USED DURING STUDY PROJECT
BY GTE SYLVANIA

1. Have any police facilities in your jurisdiction been attacked with the intent to kill or maim police personnel or to damage property?

2. If answer to No. 1 above is yes, please indicate:

2.1 By whom? (Specify group type, mob, dissidents, premeditated attack, others.)

2.2 How many involved?

2.3 Did attackers have any special skills?

2.4 What resources were available to the attackers?

2.5 Describe the attack.

2.5.1 What was the objective of the attack?

2.5.2 At what time did the attack take place?

2.5.3 What weapons or equipment did the attackers use? Effective?

2.5.4 How was the attack conducted? Coordinated, series/waves, separated actions at separate times, etc.

2.5.5 Results of attack:

3. If answer to No. 1 above is negative, why in your opinion have there been no attacks on your facilities?

4. If answer to No. 1 is yes, please provide data about types of attack, i.e., incidence, rate, frequency of successful attacks, most probable attack method, etc.

5. Have any officers or vehicles assigned to your police facilities been attacked while away from base? Please describe, using format/details listed in Question No. 2 above.

6. Police Facilities Information:

6.1 Plan-drawings/photographs depicting type of construction:

6.1.1 Parking lot, including size, capacity, layout.

6.1.2 Lighting.

6.1.3 Entrances and exists.

6.1.4 Physical deterrents (fences, walls, guards, etc.).

6.1.5 Location of personnel at various times of day.

6.1.6 Security devices and/or procedures.

6.1.7 Areas accessible to the public.

6.1.8 Description of neighborhood:

6.1.8.1 Residential - type.

6.1.8.2 Industrial - type.

6.1.8.3 Dissident groups -- describe in detail, providing information on any confrontations/demands.

6.1.9 Description of surrounding terrain.

6.1.10 Room locations -- basement, ground and upper floors:

6.1.10.1 Controlled-access areas.

6.1.10.2 Weapon storage areas.

6.1.10.3 Sealed areas.

6.1.10.4 Storage areas for evidence collected and required for future judicial action.

6.1.10.5 Communications -- type and location.

6.1.10.6 Location and distance from nearest police aid.

6.2 What do you consider to be the vulnerabilities of your facility?

6.2.1 Specific areas contributing to this vulnerability?

6.2.2 Specific area subject to what types of attack?

APPENDIX B

NBDC DATA SUMMARY

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

RESEARCH DIVISION

NATIONAL BOMB DATA CENTER

LAW ENFORCEMENT ASSISTANCE ADMINISTRATION

U. S. DEPARTMENT OF JUSTICE

[illegible] BROAD
[illegible], MARYLAND 20850
[illegible] TELEPHONE 948-0922

A CENTER FUNDED BY THE LAW ENFORCEMENT ASSISTANCE ADMINISTRATION OF THE U.S. DEPARTMENT OF JUSTICE

SIX MONTHS SUMMARY REPORT

INTRODUCTION

These statistical reports present the total United States figures for bombing incidents and related data for the period July 1 through December 31, 1970. The data was collected from data published in the public media and/or data reported to the NBDC by participating law enforcement agencies.

The statistical data has been arranged in the following six tables:

Table A--Incidents, Casualties, and Damage--By Geographic Region

Table B--Incidents, Casualties, and Damage--By Population Group

Table C--Explosive and Incendiary Devices--By Geographic Region and Population Group

Table D--Classification of Bombing Incidents by Known or Suspected Motive or Intent

Table E--Summary of Devices and Fillers

Table F--Summary of Target Location

REPORTING PERIOD JULY 1, 1970 THROUGH DECEMBER 31, 1970

	EXPLOSIVE		INCENDIARY		TOTALS
	Detonation	No Detonation	Ignition	No Ignition	
INCIDENTS	302	76	352	34	764
BOMBS	352	92	471	76	991
INJURIES	52		30		82
DEATHS	7		3		10

Table A

This table displays, by nine geographic regions, data on bomb incidents for this reporting period. A bomb incident may involve more than one explosive device. The actual number of incendiary or explosive devices is shown in tables C through F.

Table A uses the data reported for each region and displays it according to the following categories:

1. Incidents. Number of explosive or incendiary incidents reported, indicating also those incidents in which a device functioned.

2. Casualties. Number of injuries and deaths in three categories:

   a. Non-police
   b. Police (law enforcement)
   c. Bombing suspects

3. Property Damage. The amount of property damage and the number of incidents for which damage was reported. The number of incidents for which property damage was not reported is also indicated.

The following is a list of the U. S. geographic regions and their population used in table A as reported in Statistical Abstract of the United States--1968.

Region	Population 1968 Data
New England	11,450,000
Middle Atlantic	36,900,000
East North Central	39,599,000
West South Central	19,009,000
West North Central	16,061,000
South Atlantic	30,001,000
East South Central	13,098,000
Pacific	25,638,000
Mountain	7,907,000

Table B

Table B follows the same format as table A but arranges the statistical data by seven population groups and a category for incidents in which the population group was not reported.

Below is a table which provides the number of places, total population, and percentage of population for each population group. The 1970 estimate was arrived at by taking the 1960 population percentages and multiplying by the 1970 official total population of 203,185 (1,000's). The exact 1970 count was 203,184,772. This data will be revised as the official 1970 census figures become available.

Population Group	Number of Places (1960)	1960 Population (1,000's)	% of Total 1960 Population	Estimated 1970 Population (1,000's)
Over 250,000	51	39,361	22.0	44,701
100,000-250,000	81	11,652	6.5	13,207
50,000-100,000	201	13,836	7.7	15,645
25,000-50,000	432	14,951	8.3	16,864
10,000-25,000	1,134	17,568	9.8	19,912
Under 10,000	4,193	18,050	10.1	20,522
Unincorporated *	13,749	63,905	35.6	72,334
TOTALS	19,790	179,323	100.0	203,185

* Includes unincorporated urban population and total rural population.

Table C

Table C follows the format of tables A & B, but lists the number of devices reported rather than the number of incidents.

Table D

Table D gives a breakdown of statistical data on motivation and/or intent for bombing incidents during the reporting period and to date. The data is presented both for incidents and devices.

Table E

Table E presents data on the type of devices and the type of explosive or incendiary filler material used. This table lists six major categories for type of device with various subcategories. Table E also lists eight major categories for type of filler material with numerous subcategories.

Table F

Table F identifies target locations for the incidents during the reporting period. This data is arranged in five major categories, with numerous subcategories under the major headings.

TABLE A

Incidents, Casualties, and Damage — By Geographic Region

GEOGRAPHIC REGION	NUMBER OF BOMB INCIDENTS REPORTED						BOMBING CASUALTIES						ESTIMATED PROPERTY DAMAGE		
	Explosives		Incendiaries		Total		Non-Police		Police		Bombing Suspects		Reported		Incidents not Reporting Estimated Damage
	Detonations	Non Detonations	Ignitions	Non Ignitions	Function	Non Function	Injured	Killed	Injured	Killed	Injured	Killed	Number	Amount	
NEW ENGLAND Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont	19	7	39	4	58	11	1				5	1	21	$160,000	48
MIDDLE ATLANTIC New Jersey, New York, Pennsylvania, Puerto Rico, Virgin Islands	45	14	85	3	130	17	9		1		1		27	1,332,900	120
EAST NORTH CENTRAL Illinois, Indiana, Michigan, Ohio, Wisconsin	79	16	90	9	169	25	27	2			1	1	71	2,696,564	123
WEST SOUTH CENTRAL Arkansas, Louisiana, Oklahoma, Texas	11	1	6		17	1	2				1		5	36,410	13
WEST NORTH CENTRAL Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota	36	9	21	5	57	14	6	1	11	1	2	1	22	527,170	49
SOUTH ATLANTIC Delaware, Florida, Georgia, Maryland, North Carolina, South Carolina, Virginia, West Virginia, Washington, D.C.	28	8	57	6	85	14	3				4		29	151,960	70
EAST SOUTH CENTRAL Alabama, Kentucky, Mississippi, Tennessee	8	3			8	3					1	1	2	20,000	9
PACIFIC Alaska, California, Hawaii, Oregon, Washington	65	16	44	7	109	23	5	2	1				68	890,335	64
MOUNTAIN Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, Wyoming	11	2	10		21	2	1						14	97,950	9
U.S. TOTALS	302	76	352	34	654	110	54	5	13	1	15	4	259	$5,913,289	505

7/70-12/70

TABLE B
Incidents, Casualties, and Damage — By Population Group

POPULATION GROUP	NUMBER OF BOMB INCIDENTS REPORTED						BOMBING CASUALTIES						ESTIMATED PROPERTY DAMAGE		
	Explosives		Incendiaries		Total		Non-Police		Police		Bombing Suspects		Reported		Incidents not Reporting Estimated Damage
	Detonations	Non Detonations	Ignitions	Non Ignitions	Function	Non Function	Injured	Killed	Injured	Killed	Injured	Killed	Number	Amount	
I. OVER 250,000	127	36	116	8	243	44	38	4	10	1	2	2	97	$1,971,540	190
II. 100,000 to 250,000	30	9	47	8	77	17	4	1			5	1	28	1,989,219	66
III. 50,000 to 100,000	17	6	42	3	59	9	3						25	386,910	43
IV. 25,000 to 50,000	37	12	56	6	93	18	6				3	1	44	355,495	67
V. 10,000 to 25,000	36	6	30	5	66	11	2				3		24	674,425	53
VI. UNDER 10,000	41	2	48	4	89	6			2				29	279,140	66
VII. UNINCORPORATED AREA	7	2	7		14	2	1				1		8	5,810	8
VIII. UNKNOWN	7	3	6		13	3			1		1		4	250,300	12
U.S. TOTALS	302	76	352	34	654	110	54	5	13	1	15	4	259	5,913,289	505

7/70-12/70

TABLE C
Explosive and Incendiary Devices — By Geographic Region and Population Group

GEOGRAPHIC REGION	NUMBER OF BOMBS REPORTED					
	Explosive		Incendiary		Total	
	Detonations	Non Detonations	Ignitions	Non Ignitions	Function	Non Function
NEW ENGLAND Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont	19	7	68	7	87	14
MIDDLE ATLANTIC New Jersey, New York, Pennsylvania, Puerto Rico, Virgin Islands	46	16	116	21	162	37
EAST NORTH CENTRAL Illinois, Indiana, Michigan, Ohio, Wisconsin	82	22	105	20	187	42
WEST SOUTH CENTRAL Arkansas, Louisiana, Oklahoma, Texas	46	1	7		53	1
WEST NORTH CENTRAL Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota	41	12	25	8	66	20
SOUTH ATLANTIC Delaware, Florida, Georgia, Maryland, North Carolina, South Carolina, Virginia, West Virginia, Washington, D.C.	31	9	73	7	104	16
EAST SOUTH CENTRAL Alabama, Kentucky, Mississippi, Tennessee	9	3			9	3
PACIFIC Alaska, California, Hawaii, Oregon, Washington	67	20	66	13	133	33
MOUNTAIN Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, Wyoming	11	2	11		22	2
U.S. TOTALS	352	92	471	76	823	168

POPULATION GROUP	NUMBER OF BOMBS REPORTED					
	Explosive		Incendiary		Total	
	Detonations	Non Detonations	Ignitions	Non Ignitions	Function	Non Function
I. OVER 250,000	129	43	146	31	275	74
II. 100,000 to 250,000	30	9	71	17	101	26
III. 50,000 to 100,000	19	10	53	7	72	17
IV. 25,000 to 50,000	81	13	79	9	160	22
V. 10,000 to 25,000	36	10	36	7	72	17
VI. UNDER 10,000	43	2	68	5	111	7
VII. UNINCORPORATED AREA	7	2	7		14	2
VIII. UNKNOWN	7	3	11		18	3
U.S. TOTALS	352	92	471	76	823	168

7/70-12/70

TABLE D

Classification of Bombing Incidents
By Known or Suspected Motive or Intent

THIS REPORTING PERIOD		MOTIVATION/INTENT CLASSIFICATION		SINCE 1 JULY 70	
DEVICES	INCIDENTS			DEVICES	INCIDENTS
15	14	0X	NONE, ACCIDENTAL	15	14
497	401	0Y	UNKNOWN	497	401
		01	ASSASSINATION, POLITICAL		
		02	ASSASSINATION, RACIAL/RELIGIOUS		
		03	ASSASSINATION, LABOR/MANAGEMENT		
13	13	04	DIVERSION, CRIMINAL ACTIVITY	13	13
1	1	05	EXTORTION	1	1
		06	HOMICIDE, OTHER		
1	1	07	INSURANCE FRAUD, PROPERTY	1	1
		08	INSURANCE FRAUD, LIFE		
1	1	09	INTIMIDATION, WITNESS/JUROR	1	1
91	60	10	JUVENILE VANDALISM	91	60
4	4	11	JEALOUSY	4	4
48	45	12	PROTEST, POLITICAL	48	45
99	48	13	PROTEST, RACIAL	99	48
15	15	14	PROTEST, ANTI-WAR	15	15
59	46	15	PROTEST, OTHER	59	46
39	29	16	REVENGE	39	29
		17	SUICIDE		
11	5	18	ENTRAPMENT, PUBLIC SAFETY PERSONNEL	11	5
51	38	19	PUBLIC SAFETY HARASSMENT	51	38
46	43	0Z	OTHER	46	43
991	764		TOTALS	991	764

7/70-12/70

TABLE E
Summary of Devices and Fillers

TYPE OF DEVICE

1. EXPLOSIVE (Non-Military) — 412
   - A. Blast Only 229
   - B. Blast and Fragmentation 111
   - C. Shaped Charge
   - Z. Other 23
   - Y. Unknown 49
2. INCENDIARY (Non-Military) — 545
   - A. Liquid 538
   - B. Jelled
   - C. Solid 1
   - Z. Other
   - Y. Unknown 6
3. COMBINATION (Non-Military) — 14
   - A. Explosive/Incendiary 14
4. U.S. MILITARY ORDNANCE — 15
   - A. Explosive 14
   - B. Incendiary 1
5. FOREIGN MILITARY ORDNANCE
   - A: Explosive
   - B. Incendiary
6. OTHER — 5

EXPLOSIVE/INCENDIARY MATERIAL

1. EXPLOSIVE (Non-Military) — 374
   - A. Dynamite 104
   - B. Black Powder 38
   - C. Smokeless Powder 11
   - D. Ammonium Nitrate 1
   - E. Liquid 2
   - F. Potassium Chlorate 1
   - G. Blasting Primers or Boosters
   - H. Nitroglycerin 1
   - Z. Other 45
   - Y. Unknown 171
2. INCENDIARY (Non-Military) — 546
   - A. Gasoline 182
   - B. Gasoline Mixture 23
   - C. Lp Gas
   - D. Other Flammable Liquid 22
   - E. Sugar Chlorate Mix
   - F. Match Heads
   - G. Flare Fireworks 2
   - H. Other Flammable Solid
   - I. Other Flammable Jell
   - Y. Unknown 317
3. COMBINATION (Non-Military) — 17
   - A. Explosive/Incendiary 15
   - B. Explosive Explosive 2
   - C. Incendiary/Incendiary
   - Y. Unknown
4. MILITARY EXPLOSIVES — 51
   - A. TNT
   - B. Dynamite
   - C. Plastic 40
   - Z. Other 7
   - Y. Unknown 4
5. MILITARY INCENDIARY — 1
6. COMBINATION (Military and Non-Military)
   - A. Explosive Incendiary
   - B. Explosive Explosive
   - C. Incendiary Incendiary
7. FOREIGN — 2
   - A. Explosive 2
   - B. Incendiary
   - Y. Unknown
8. OTHER

7/70-12/70

TABLE F
Summary of Target Location

LOCATION OF DEVICE		LOCATION OF DEVICE		LOCATION OF DEVICE	
VEHICLE	75	**COMMERCIAL MANUFACTURING**	294	**JUDICIAL FACILITY**	6
01 Automobile 35		40 Office building 38		80 Judicial, local 3	
02 Truck 3		41 Department store 34		81 Judicial, county 3	
03 Bus 37		42 Bank 35		82 Judicial, state	
04 Train		43 Radio station 2		83 Judicial, federal	
05 Subway		44 Gasoline station 8		89 Other judicial facility	
06 Aircraft, private		45 Garage 6			
07 Aircraft, commercial		46 Warehouse 10		**POLICE FACILITY**	67
08 Ship/boat, private		47 Manufacturing plant 29		90 Headquarters 8	
09 Ship/boat, commercial		49 Other commercial/mfg. 132*		91 District station 5	
10 Other vehicle				92 Vehicle(s) 25	
		TRANSPORTATION FACILITY	18	93 Motor pool 1	
RESIDENCE	192	50 Dock		94 Communications facility	
11 Private home 152		51 Airport		95 Officers' home/personal vehicle 13	
12 Apartment 33		52 Bus terminal 1		98 Other police 15	
13 Hotel 2		53 Train terminal 1			
14 Motel 3		54 Bridge 1		**MILITARY FACILITY**	24
19 Other residence 2		55 Tunnel			
		56 Highway 9		**RELIGIOUS FACILITY**	21
EDUCATIONAL INSTITUTION	102	57 Intersection 1			
20 College/University 22		59 Other transportation 5		**IN STORAGE/TRANSPORT**	8
21 High school 63					
22 Grade school, public 12		**RECREATION FACILITY**	61	**UNKNOWN**	18
23 Grade school, private 1		60 Restaurant 22			
29 Other educational 4		61 Bar/tavern/club 15		**OTHER**	21
		62 Sports stadium 1			
GOVERNMENTAL FACILITY, NON-POLICE	68	63 Theatre 2		Miscellaneous 10	
30 Government, local 20		69 Other recreational 21		Open spaces 6	
31 Government, county 15				Monument 1	
32 Government, state 2		**UTILITY**	16	Vacant structure 4	
33 Government, federal 18		70 Power station			
39 Other government 13		71 Water works 2			
		72 Fuel tank farm 2			
		73 Pipeline 2			
		79 Other utility 10			

*See reverse side for further analysis of "Other commercial/mfg."

TABLE F (cont.)

49 Other commercial

- A. Food store 20
- B. Drug store/pharmacy 9
- C. Lumberyard 6
- D. Liquor store 5
- E. Laundry/dry cleaning shop 5
- F. Barber shop 4
- G. Specialty store 26
- H. Automobile sales/etc. 11
- I. Other 46

PREVIOUS BOMB STATISTIC STUDIES

In order to provide information on bombing incidents prior to the establishment of the National Bomb Data Center in July, 1970, the following sets of tables are presented. These tables were prepared by, or at the request of, the Permanent Subcommittee on Investigations of the Committee on Government Operations of the United States Senate, of the Ninety-First Congress.

Tables G and H were compiled by the staff of the Permanent Subcommittee and list bombing incidents recorded during the period January 1, 1969 to July 9, 1970. This study was developed, for the most part, from available public source material, news clips, and a limited contact with major law enforcement agencies.

Incidents listed in tables I and J are the result of a survey conducted by the Alcohol, Tobacco and Firearms Division of the Internal Revenue Service pursuant to a request by the Permanent Subcommittee. These statistics were collected from state and local law enforcement agencies and cover the period January 1, 1969 to April 15, 1970.

TABLE G

STATISTICAL SUMMARY OF BOMBINGS AND ATTEMPTED BOMBINGS IN THE UNITED STATES DURING THE PERIOD JANUARY 1, 1969-JULY 9, 1970

TOTAL BOMBINGS AND ATTEMPTED BOMBINGS FOR CY 1969 AND CY 1970 (TO JULY 9th) BY MONTH AND TYPE OF BOMB USED

CALENDAR YEAR	EXPLOSIVE BOMBING INCIDENTS	INCENDIARY BOMBING INCIDENTS	TOTAL BOMBING INCIDENTS	TOTAL BOMBING ATTEMPTS	TOTAL BOMBING INCIDENTS/ ATTEMPTS
CY 1969					
January	24	15	39	6	45
February	34	10	44	4	48
March	28	12	40	4	44
April	31	25	56	7	63
May	30	42	72	7	79
June	28	27	55	2	57
July	26	45	71	2	73
August	15	14	29	3	32
September	20	12	32	9	41
October	22	28	50	3	53
November	24	8	32	9	41
December	16	5	21	5	26
CY 1969 TOTALS	298	243	541	61	602 1/
CY 1970					
January	40	11	51	5	56
February	37	15	52	8	60
March	53	20	73	11	84
April	66	30	96	22	118
May	69	80	149	17	166
June	24	39	63	6	69
July	12	15	27	6	33
CY 1970 TOTALS	301	210	511	75	586 2/
CY 1969-70 TOTALS	599	453	1,052	136	1,188 3/

FOOTNOTE: (For the bombings and attempted bombings covered in this study)

1/ Average bombings and attempted bombings per day in CY 1969--1.6

2/ Average bombings and attempted bombings per day in CY 1970--3.1

3/ Average bombings and attempted bombings per day for CY 1969-70--2.1

TABLE H

TOTAL BOMBINGS AND ATTEMPTED BOMBINGS
FOR CY 1969 AND CY 1970 TO JULY 9
BY CATEGORIES OF PROPERTY

CALENDAR YEAR	TOTAL BOMBING INCIDENTS ATTEMPTS	FOREIGN EMBASSIES & CONSULATES	FEDERAL GOV'T PROPERTY	STATE & MUNICIPAL GOV'T PROPERTY	INDUSTRIAL, PUBLIC UTILITIES & RAILROADS	LOCAL SMALL BUSINESS	HOMES & PERSONAL PROPERTY	SCHOOLS AND COLLEGES	CHURCHES AND SYNAGOGUES
CY 1969	602		35	56	92	114	162	124	19
CY 1970	586	7	71	70	59	139	123	104	13
CY 1969-70 TOTALS	1,188	7	106 1/	126	151	253	285 2/	228 3/	32

FOOTNOTES:

1/ Federal Government Property includes Selective Service Offices and ROTC Buildings.

2/ Of the 285 explosions involving personal property, 16 were attributed to teenagers injured in the act of constructing homemade bombs in their homes.

3/ Of the 228 explosions involving schools & colleges, 145 occurred at colleges, 71 at high schools, 7 at junior high schools, and 5 at elementary schools.

TABLE I

RECAP OF BOMBING STATISTICS, PERIOD OF JAN. 1, 1969, THROUGH APR. 15, 1970

[Statistics supplied by State and local law enforcement agencies]

	Explosive bombings	Incendiary bombings	Total bombings	Attempted bombings	Bombing threats	Property damage (in millions of dollars)	Personal injury	Deaths
Western region:								
Alaska	1	0	1	1	41	153	0	0
Arizona	3	2	5	15	178	----------	0	0
California (less southern judicial district)	109	358	467	303	2,544	2,432	1	1
Idaho	0	0	0	0	0	0	0	0
Montana	8	3	11	3	71	82	1	1
Nevada	5	28	33	5	176	25	0	0
Oregon	18	78	96	16	382	144	2	0
Washington	90	80	170	27	452	442	3	5
Southern judicial district of California [1]	[1] (76)	[1] (924)	[1] (1,000)	----------	[1] (2,880)	(1)	[1] (5)	[1] (1)
Utah	1	1	2	1	[1] (79)	[1] (1)	----------	----------
Grand total	235	550	785	371	3,844	3,278	7	7
Southwest region:								
Arkansas	0	66	66	6	62	66	0	0
Colorado [1]	[1] (97)	[1] (167)	[1] (264)	[1] (27)	[1] (486)	[1] (707)	[1] (2)	----------
Kansas	12	14	26	3	293	40	0	0
Louisiana	42	19	61	67	1,367	538	0	0
New Mexico	5	5	10	9	24	365	0	0
Oklahoma	10	9	19	3	232	60	1	0
Texas	40	44	84	43	861	739	3	5
Wyoming	4	0	4	1	16	1	0	0
Grand total	113	157	270	132	2,855	2,809	4	5
Southeast region:								
Alabama	5	83	88	3	549	38	0	0
Florida	30	194	224	5	987	221	2	2
Georgia	9	1	10	4	235	20	1	1
Mississippi	13	12	25	13	159	28	0	0
North Carolina	27	130	157	72	941	2,155	2	0
South Carolina	0	0	0	1	23	0	0	0
Tennessee	9	17	26	11	434	552	0	0
Grand total	93	437	530	109	3,328	3,014	5	3
Midwest region:								
Illinois	29	626	655	32	721	14	0	0
Iowa	75	105	180	174	375	1,500	0	0
Minnesota	3	0	3	0	105	7	0	0
Missouri	38	103	141	8	640	75	11	0
Nebraska	16	43	59	59	211	315	2	0
North Dakota	0	0	0	0	6	0	0	0
South Dakota	1	0	1	0	14	0	0	0
Wisconsin	2	10	12	0	260	1	0	0
Grand total	164	887	1,051	273	2,332	1,912	13	0
Central region:								
Indiana	10	76	86	11	625	643	0	0
Kentucky	57	25	82	10	397	948	4	0
Michigan	27	356	383	95	2,492	355	165	7
Ohio [2]	28	105	133	62	1,767	1,163	2	1
West Virginia	2	10	12	5	109	35	1	0
Grand total	124	572	696	183	5,390	3,144	172	8
Mid-Atlantic region:								
Delaware	1	2	3	2	20	255	1	0
Maryland	4	12	16	2	240	43	0	2
New Jersey	16	39	55	20	803	890	2	0
Pennsylvania	41	226	267	81	1,119	3,192	15	5
Virginia (District of Columbia)	6	90	96	12	440	146	0	0
Grand total	68	369	437	117	2,622	4,526	18	7

TABLE I (cont.)

	Explosive bombings	Incendiary bombings	Total bombings	Attempted bombings	Bombing threats	Property damage (in millions of dollars)	Personal injury	Deaths
North Atlantic region:								
Connecticut	11	39	50	30	1,267	1,565	23	0
Maine	5	7	12	0	136	16	0	1
Massachusetts	31	55	86	80	2,941	262	1	0
New Hamphsire	6	0	6	1	181	1	0	1
New York	121	177	298	163	9,412	2,000	106	8
Rhode Island	4	105	109	16	668	311	35	0
Vermont	0	0	0	0	153	0	0	0
Grand total	178	383	561	290	14,758	4,155	165	10
National total	975	3,355	4,330	1,475	35,129	21,838	384	40

[1] Figures in parentheses supplied by police officials in the area making up the Southern Federal Judicial District of California and Colorado were for the years 1968, 1969 and 3 months of 1970. They cannot be broken down by year and are not included in the grand total for the Western region, Southwest region or the national total.

[2] Not included in the total of 133 bombings are 67 bombings which data from respective police agencies did not identify as either explosive or incendiary in nature. As a result total bombings for Ohio are actually 200.

TABLE J

ACTUAL BOMBINGS, ATTEMPTS AND THREATS—BY REGIONS

	Western	North Atlantic	Southwest	Southeast	Midwest	Central	Mid-Atlantic	National Totals
Explosive	235	178	113	93	164	124	68	(173) 975
Incendiary	550	383	157	437	887	572	369	(1,091) 3,355
Total actual bombings	785	561	270	530	1,051	696	437	(1,264) 4,330
Bombing attempts	371	290	132	109	273	183	117	1,475
Bombing threats	3,844	14,758	2,855	3,328	2,332	5,390	2,622	35,129

#0392

CCCJ No. 0392 Sub-Grantee: City & Co. of San Francisco P.D.

Project Title: S.F. Police Station Security System Study

Period of Funding: 1/1/71 - 8/13/71 $69-70 Year of Funding

Task Force: Pol. Ser Program:

Quarterly Progress Report	On-Site Monitoring Visits	Final Evaluation Report Final report
No. Submitted:	No. Visits:	Date Rec'd:
Period Covered by Each Report:	Date of Visits:	8/71
		Period Covered:
	Written By:	
5/1/71 8/13/71		

#0392

FINAL PROGRESS REPORT

SAN FRANCISCO POLICE DEPARTMENT SECURITY STUDY

#0392

The San Francisco Police Department Security Study has been completed. Drafts of the final report were distributed to the Advisory Committee members in early August for review and comment.

The report provides detailed discussion of the various subelements of an integrated security system and their interrelationships. The requirements for a police-facility security system were established, and cost-effective security subsystems were selected for use in negating the threats. Some of the more salient recommendations are listed below.

a. Keep security monitor apprised of all activity in and around the facility.

b. Provide physical security to keep the public away from the outside of the building and away from police vehicles.

c. Provide systems to detect intrusions across or through the perimeter fence, through gate areas, through all doors leading into the building, and on flat roof areas.

d. Provide an easily implemented scheme for identification of authorized personnel in areas surrounding the building.

e. Provide a method of easily installing detection systems and monitoring their outputs.

f. Deny places of easy concealment of explosives by keeping shrubbery and trash away from building for easy surveillance and the denial of good bomb implantation locations.

g. Deny visual access to snipers by filling in all windows except those required for surveillance. Surveillance windows should be of a bullet-resistant material.

h. Public access must be controlled at all times. The public should be allowed to enter the inner part of the facility only if escorted by an authorized person.

In general, all of the systems recommended are simple, reliable and flexible, consistent with the requirements of the application. For example, no need was identified for the use of a sophisticated volumetric detection system. The majority of detection devices in the facilities will be magnetic switches and beam-breakers - reasonable in cost, easy to install and to maintain. It is further recommended, however, that the continuous-line vibration sensor be used to detect intrusions through or over the perimeter fence and on flat roofs.

The system recommended for transmission of the alarm from the detection device to a monitoring point provides for maximum flexibility and ease of installation. The detection device interfaces with a remote alarm transmitter which is simply plugged into the nearest AC power outlet. The AC lines, themselves, are used for the transmission of alarms. This means that there is no need to run wire from point-to-point, since existing power lines are being used. All that is required to relocate either the remote alarm transmitters or the Displays is to simply plug it in at the new location.

Another system which is recommended assists in the discrimination of authorized from unauthorized intrusions. During the operation of the facility, there will be many "intrusions" created by entry of authorized personnel into the limited-access area surrounding the building. It is highly desirable from a standpoint of good area control that some method be used to discriminate these intrusions. The method recommended is to electronically monitor all intrusions into the area (over or through the fence or through gates). Any intrusions over or through the fence, of course, can be automatically classified as an unauthorized intrusion. Intrusions through the gates, however, must be discriminated. This can be done through a cooperative method. Each authorized individual is given a small coded transmitter. The codes on the transmitter can be easily changed from day to day. Since a long-wire antenna can be looped around the building, the transmitters can be quite simple since they only have to transmit a distance of a few feet. An authorized intruder knows that he is being detected as he enters the gate. He also knows that within some predetermined time after the intrusion (of the order of 5 seconds), he must identify himself by depressing the button on his transmitter. If he does this and his transmitter has the proper code, no alarm will be generated. If, however, the intruder has a wrong code or no identification transmitter at all, then an alarm will be generated and displayed on the security monitoring console. The monitoring personnel then know that an unauthorized person is in the limited-access area surrounding the facility and can take the appropriate action.

In addition to the above electronic equipment to assist the security monitor, there are a variety of physical security devices which are recommended for use in police facilities. These consist of fences, gates (remote controlled and manual), electric locks, bullet-resistant glass, physical and visual barriers, mirrors, and combination locks. These physical devices are very important to the operation of the overall integrated security system. They should be the first to be installed in any facility. The report details the recommended use of the above physical security equipment.

Copies of the final report will be ready for distribution in the second week of September.

END