Law Enforcement Equipment Technology

Selection and Application Guide to COMMERCIAL INTRUSION ALARM SYSTEMS

NBS SPECIAL PUBLICATION 480-14

A USER GUIDE FROM THE NATIONAL BUREAU OF STANDARDS

ACKNOWLEDGMENTS

This guide was prepared by the Law Enforcement Standards Laboratory of the National Bureau of Standards under the direction of Lawrence K. Eliason, Manager, Security Systems Program, and Jacob J. Diamond, Chief of LESL. Its preparation was sponsored by the National Institute of Law Enforcement and Criminal Justice, Lester D. Shubin, Standards Program Manager.

Selection and Application Guide to Commercial Intrusion Alarm Systems

NBS Special Publication 480-14

by
Dr. A. H. Sher
Gerard N. Stenbakken
Center for Electronics and
Electrical Engineering
National Bureau of Standards

and the
Law Enforcement Standards Laboratory
Center for Consumer Product Technology
National Bureau of Standards
Washington, D.C. 20234

prepared for
National Institute of Law Enforcement
and Criminal Justice
Law Enforcement Assistance Administration
U.S. Department of Justice
Washington, D.C. 20531

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary
Luther H. Hodges, Jr., Under Secretary
Jordan J. Baruch, Assistant Secretary for Science and Technology
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Director

Issued August 1979

Library of Congress Cataloging in Publication Data

Sher, Alvin H.

Selection and application guide to commercial intrusion alarm systems.

(NBS special publication ; 480-14)

Supt. of Docs. no.: C 13.10:480-14

I. Burglar-alarms—Handbooks, manuals, etc. I. Stenbakken, Gerard N., joint author. II. Law Enforcement Standards Laboratory. III. National Institute of Law Enforcement and Criminal Justice. IV. Title. V. Series: United States. National Bureau of Standards. Special publication ; 480-14.

QC100.U57 no. 480-14 [TH9739] 602'1s 78-21624

[621.389'2]

National Bureau of Standards

Special Publication 480-14

Nat. Bur. Stand. (U.S.), Spec. Publ. 480-14; 40 pages

CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON: 1979

For sale by the Superintendent of Documents

U.S. Government Printing Office, Washington, D.C. 20402

(Order by SD Catalog No. C13.10:480-14) Stock No. 003-003-02098-2

(Add 25 percent additional for other than U.S. mailing).

CONTENTS

FOREWORD

The Law Enforcement Standards Laboratory (LESL) of the National Bureau of Standards (NBS) furnishes technical support to the National Institute of Law Enforcement and Criminal Justice (NILECJ) program to strengthen law enforcement and criminal justice in the United States. LESL's function is to conduct research that will assist law enforcement and criminal justice agencies in the selection and procurement of quality equipment.

LESL is: (1) Subjecting existing equipment to laboratory testing and evaluation and (2) conducting research leading to the development of several series of documents, including national voluntary equipment standards, user guides, and technical reports.

This document is a law enforcement equipment guide developed by LESL under the sponsorship of NILECJ. Additional guides as well as other documents are being issued under the LESL program in the areas of protective equipment, communications equipment, security systems, weapons, emergency equipment, investigative aids, vehicles and clothing.

Technical comments and suggestions concerning this guide are invited from all interested parties. They may be addressed to the authors or to the Law Enforcement Standards Laboratory, National Bureau of Standards, Washington, D.C. 20234.

Jacob J. Diamond
Chief, Law Enforcement
Standards Laboratory

INTRODUCTION

Crimes against businesses, small and large, are a commonplace occurrence and, regrettably, security has become essential in the operation of any business. With the increase in burglary, more and more businesses are turning to alarm systems for increased protection. The selection of a suitable alarm system is not a simple matter. You are faced with a wide and possibly confusing array of equipment and services. For guidance, you could: a) Read the numerous excellent textbooks on intrusion alarm systems—if you have the time; b) utilize the services of consultants in the field—if the size of your business warrants it; c) rely solely upon the recommendations of alarm system dealers and installers—who may have only a specific product line or type of equipment to offer; or d) study the innumerable articles in the popular trade press—which may not give you enough information for your specific needs. This guide is intended to provide an alternate means for you to gain a general understanding of intrusion alarm systems and their potential use in your business.

The factors which determine the requirements of an individual alarm system and the questions which must be answered when selecting a system include:

- The threat—What is to be protected against?
- The type of protection—What methods are available?
- The types of sensors—What should be detected?
- The method of alarm transmission—How is the signal sent and who will respond?

The purpose of this guide is to familiarize you with:

- the types of protection that intrusion alarm systems can provide,
- the manner in which they operate and
- the characteristics of the various system components as they relate to different applications.

The basic considerations that determine your individual needs are discussed in general terms, thus enabling you to more effectively deal with and understand the services of the many reputable alarm system companies that are ready to serve your needs.

The Law Enforcement Standards Laboratory (LESL) is continuing to develop performance standards for intrusion alarm components. Equipment that meets the requirements of these individual standards will provide reliable performance with a minimum of false alarm susceptibility. In addition, LESL has prepared a number of guides and reports concerning security equipment and systems that you will find to be useful companion documents to this guide*.

An intrusion alarm may sometimes serve to deter a would-be intruder. However, the primary function of the system is to signal the presence of the intruder. An intrusion alarm system is only part of the overall protection needed; many large businesses will supplement them with guards and other security personnel, and even the smallest will have a locked door. In addition, it is important for you to recognize that the successful operation of a system depends upon not only the system equipment but also upon its proper installation, maintenance, and use.

*A list of all current LESL publications is available upon request from the Law Enforcement Standards Laboratory, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C. 20234.

When you are deciding whether to install an intrusion alarm system, cost cannot be the sole basis for your decision.

BASIC CONSIDERATIONS

Economics

As a businessman, you must consider the economic aspects of your decision as to whether or not to install an intrusion alarm system, since the acquisition and operation of the system will undoubtedly be reflected in your overhead. However, an intrusion alarm system has safety as well as economic aspects, and cost cannot be the sole criterion upon which your decision is made. You may wish to install an intrusion alarm primarily for the peace of mind that it affords you or your employees.

Intrusion alarm systems have been demonstrated to be effective. In a typical study, the intruder apprehension rate for protected premises was six times that for unprotected premises. Obviously, the chances of recovering your property are proportional to the apprehension rate, particularly if the intruder is taken into custody in or near your place of business. In addition, the actual dollar value of losses from a business protected by an intrusion alarm has been found to be significantly less than that of a business not protected by an alarm system. The potential deterrent value should not be

overlooked either. It is not uncommon for a burglar to avoid businesses that have intrusion alarm systems.

The choice between a local alarm system, which signals an alarm only at the protected premises, and a remote alarm system, which transmits the alarm signal to the police or a central station, will be a major factor in the operating cost. The local alarm system, least expensive, is suitable for use if the primary object of the alarm is to scare the intruder away from the premises. If the objective of the system is apprehension, a remote alarm should be employed.

Large retail businesses or industrial firms may choose to install an intrusion alarm system that transmits all alarm signals to a central location staffed by its own guards or security personnel. Such systems, referred to as proprietary systems, are obviously expensive to operate and can usually be justified only for large firms.

The economic aspects of installing an intrusion alarm system are also influenced by insurance considerations. In many instances, insurance rates are lower if the business has an intrusion alarm system. It is not uncommon for an insurance company to refuse to issue a policy to a high-risk establishment that does not have an intrusion alarm system.

If your business is located in a city or region classified by the Department of Housing and Urban Development (HUD) as a high-crime area, you should investigate your eligibility for HUD anti-crime insurance. Policies issued under this program are Federally subsidized to provide rates significantly lower than those of normal commercial insurance. It is mandatory, however, that the insured premises have an intrusion alarm system.

Depending upon the physical size of your business premises and the complexity of the intrusion alarm system that is installed, you will be faced with installation costs ranging from hundreds to thousands of dollars. In addition, service fees could range from 50 to several hundred dollars per month. Service fees vary considerably from one locality to another. When such factors as insurance rates and safety are properly accounted for, only you can determine if your potential property loss justifies the expense.

The Threat

Common crimes against businesses are burglary, arson, vandalism, and holdups. These crimes have as a common element the unauthorized presence in an establishment of one or more individuals, usually after normal business hours. Entry into the premises may be accomplished by force from the outside or by hiding inside before closing time. Generally, a large portion of those who commit such crimes are unskilled juveniles. Normally they have little education, training, or criminal expertise and select targets where special skills, planning, and training are not required to gain entry.

The potential threat to a place of business depends upon many factors. The location (high-crime area, isolated area, shopping center, etc.) of the business is a primary factor. It has been found that the incidence of burglary, robbery, and theft is highest in the inner city, less in suburban areas, and lowest in rural areas. The continued expansion of shopping centers into suburban and rural areas, however, has resulted in rapidly increasing crime rates in areas outside the central cities. The type of business will also affect the probability that it will be attacked. Leading targets for theft include jewelry, liquor, clothing, and drugs. Establishments that frequently have large amounts of cash on hand, such as banks, supermarkets, discount stores, drug/variety stores, and gasoline stations are also frequent targets. Your local law enforcement agency, or a review of its records, can often provide you with information as to the types of businesses that are most frequently attacked in your area.

The threat to your business may well encompass more than the loss of merchandise or the proceeds from sales. The malicious burglar, the vandal, or the arsonist may destroy or remove important business records, resulting in a loss of far more than the stolen cash or

merchandise. In addition, damage to the building and its contents may prevent you from conducting normal business for extended periods of time until repairs are made and new stock is obtained.

The time you devote to defining the potential threat to your business will be time well spent, for you are more likely to select an intrusion alarm system that fully meets your needs. You are also much less likely to purchase a system that is more complex and expensive than you need.

HOLDUP

BURGLARY

VANDALISM & ARSON

THE THREAT

Related Protection

Although an intrusion alarm can serve to frighten an intruder away from your business, it will not always do so. You may still suffer a loss, even though a smaller one than if you did not have that protection. Therefore, it is in your best interest to take additional measures to protect your business, since the intrusion alarm is only one element of a security system.

The first and most fundamental measure is physical protection. It is quite possible, if your business is in a low- to moderate-crime area, and not of a high-risk nature, that the installation of door assemblies which will resist the forced entry attempts of unskilled and semi-skilled burglars (in combination with suitable windows which will also resist such attacks) will provide adequate protection without the need for an intrusion alarm system. The Law Enforcement Standards Laboratory has prepared guides and standards for the physical security of doors and windows which you may find useful.

The manner in which doors and windows are installed is critical to their ability to act as physical barriers to an individual attempting to break in. The installation of doors and windows is also important with respect to intrusion alarm systems, for if they are loose fitting, certain types of alarm switches installed upon them will produce frequent false alarms.

There are many other measures, not requiring a major investment, that you can take to augment an intrusion alarm system. Most are a matter of good security procedures. Remove all cash from cash registers at night. Leave the register

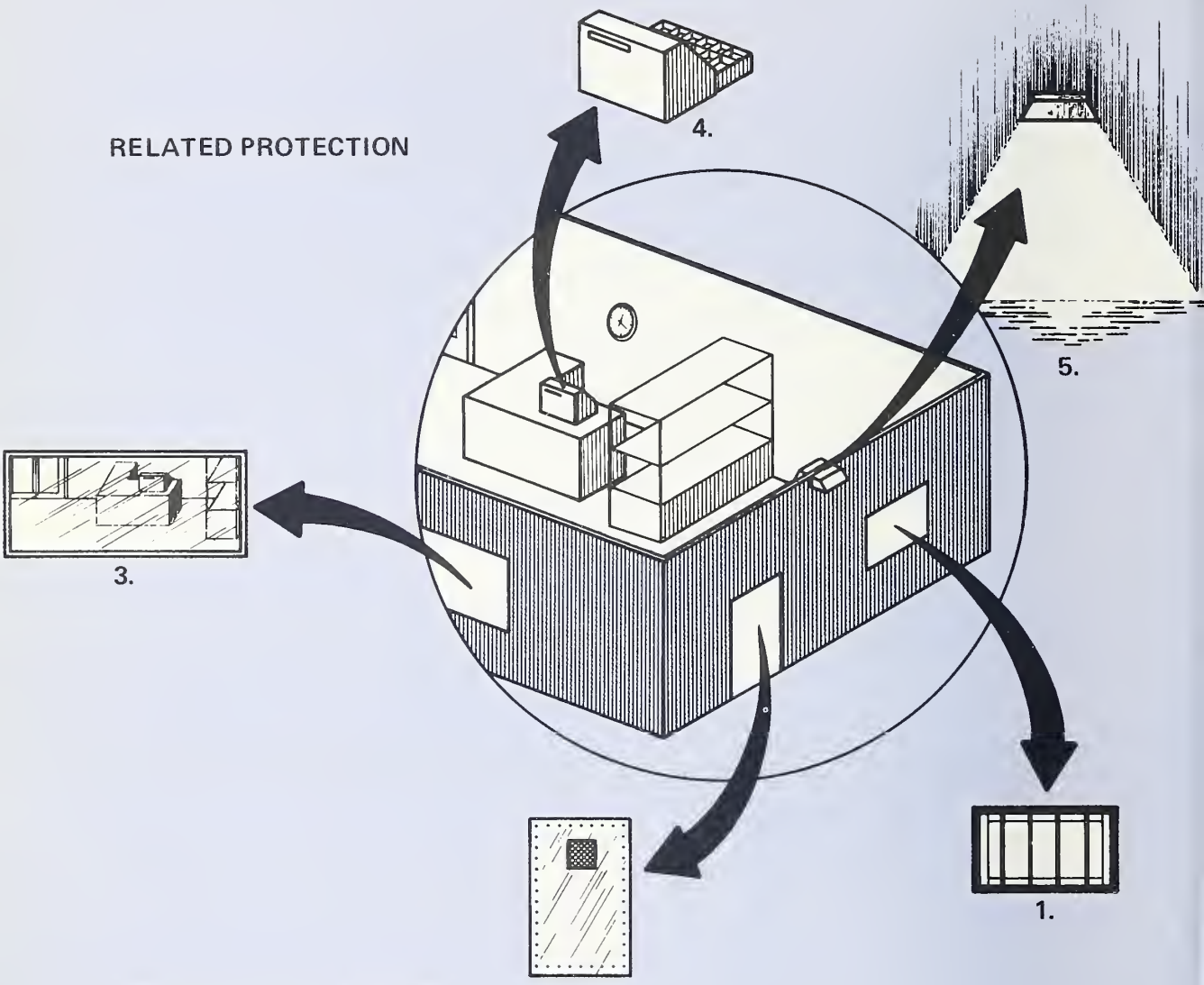
LOCATION

BUSINESS

FACTORS DETERMINING THREAT

CASH ON HAND

RELATED PROTECTION



1. INTRUSION-PROOF WINDOWS
2. INTRUSION-PROOF DOORS
3. WINDOWS CLEAR (allows police or passerby to see in)
4. CASH REGISTER DRAWER (with no money) OPEN & LIGHTED
5. LIGHTS, INSIDE & OUT, ON

Since an intrusion alarm system is only one element of a security system, it is in your own best interest to take additional measures to protect your business.

drawer open with the tray visible (a light directed on it is a good idea) so that a would-be intruder can see from the outside that he will get no cash if he breaks in. Leave some lights on and keep sales banners in the windows to a minimum so that the police patrol can see into the building from the street.

It is also a good idea to provide lights that illuminate doorways, particularly rear entrances. Do not park trucks so close to the building that they could be used as hiding places or as step ladders to second floor windows. The list is endless. Needless to say, you should remember to lock the door when you leave, and turn on the alarm.

The police departments of most cities and counties have community crime prevention units. These units will be pleased to visit your business and provide a security survey of your premises at no cost to you. They will help you to identify your vulnerabilities and provide many simple common-sense suggestions that can help to improve your overall security.

False Alarms

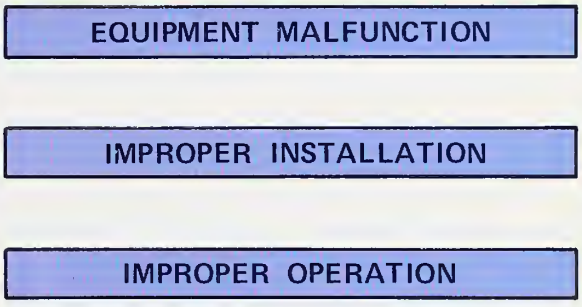
One of the most important problems associated with business intrusion alarm systems is the high incidence of false alarms. More than nine out of ten alarm signals are false alarms, with no evidence of actual or attempted forced entry. A continued high rate of false alarms from your equipment could cause the police to place a low priority on response to your alarm, since they would take it for granted that it was just another false alarm. Many local jurisdictions are seriously concerned over the time and resources wasted on officers responding to false alarms. As a result, some have enacted ordinances that permit fines to be levied against businesses that allow their intrusion alarm systems to signal an excessive number of false alarms.

False alarms are also a problem with local alarms. A local alarm system that frequently sounds false alarms quickly becomes a nuisance to adjoining businesses, and the chances of a neighboring businessman calling the police to investigate an alarm are greatly reduced.

There are numerous causes of false alarms. In some instances the false alarm is the result of malfunctioning equipment. In other cases the false alarm originates in the signal transmission line. It is also true that some false alarms are in reality alarms that have been set off intentionally by a sophisticated intruder who is testing your alarm system for possible future entry or is attempting to undermine faith in your system. The improper use or installation of many types of alarm sensors can also cause false alarms.

The statistics that have been collected, however, tend to support the belief that the largest single source of false alarms is the improper operation of the system. If the system is turned on with a door or a window open, the sensor will transmit a false alarm. If you enter your store at an odd hour without first notifying the police or central station (assuming you have a remote alarm), you will transmit a false alarm.

CAUSES OF FALSE ALARMS



The largest single source of false alarms is improper operation. Buy a system you and your employees can operate properly, thus preventing false alarms.

Once you install an alarm system, it will be your responsibility to insure that you and your employees operate it so as to avoid false alarms. When you discuss your alarm system needs with an installer, keep the false alarm problem in mind and try to select a system that you feel you and your employees can control properly. You should also study your premises to become aware of those factors that could cause certain alarm sensors to transmit a false alarm. For example, some sensors will transmit an alarm signal in response to a flickering

fluorescent light that is located nearby, while others will transmit an alarm signal in response to a ringing telephone bell. You should be aware of such problems, for if a sensor is installed in a business environment that includes a source of some type of stimulus to which it is sensitive, it can be expected to generate false alarms and limit the effectiveness of your system.

THE TYPES OF PROTECTION

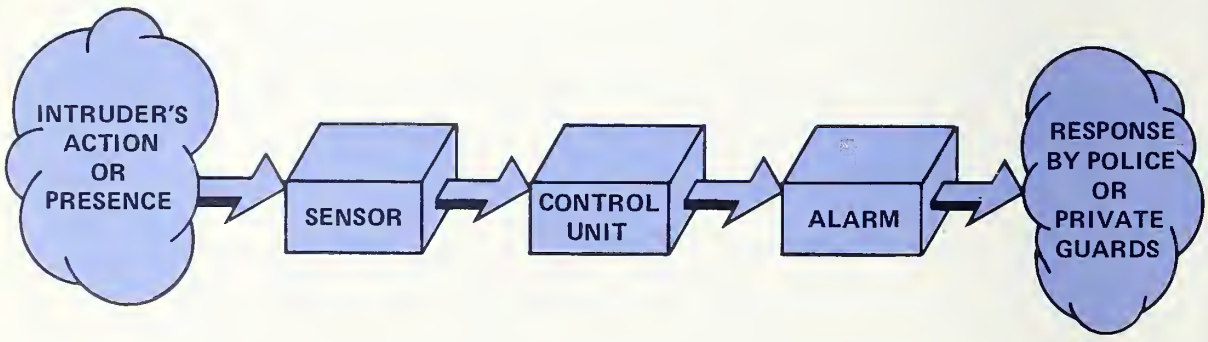
All intrusion alarm systems, from the simplest to the most complex, consist of three fundamental elements or components: a sensor which detects the action or presence of an intruder; a control unit that turns the system on and off, receives the signal from the sensor, processes the signal, and transmits the actual alarm signal; and a device to summon assistance in response to the alarm. Obviously, the system must provide a means of transmitting information between each of the functional elements. The complexity of each element varies significantly, depending upon the system.

The sensor and control unit components can be assembled into a variety of configurations to provide four basic types of protection:

- point, spot, or object
- perimeter, or linear
- area, space, or volume
- holdup

The types of protection that you select depend upon the threat to your business. Any or all of the basic types of protection can be combined to make up the sensor/control unit subsystem.

If you have the idea that it would be possible to combine the four types of protection in literally a hundred different ways for a single establishment, you are absolutely right. The design of an intrusion alarm system is further complicated because in many cases there are several different types of sensors from which to choose. Of course, there are many manufacturers of sensors and components, each with products containing features that distinguish his products from his competitors'. For this reason, you can expect that no two alarm installers will propose to install exactly the same system. You can, however, take comfort in the fact that the general approach to protection will be similar, leaving you to judge the advantages or disadvantages of only a few features.



All intrusion alarm systems consist of three fundamental elements: a sensor which detects the action or presence of an intruder; a control unit which turns the system on and off, receives the signal from the sensor, processes the signal, and transmits the actual alarm signal; and an alarm which summons assistance in response to the alarm signal.

In many cases, the alternatives offered by different alarm installers will be a consequence of individual sources of supply. In every case, the reputable alarm company will make its recommendation based upon experience with a specific sensor or item of equipment, and should know how well it can be expected to perform in your application. Do not hesitate to ask for the names of other businesses that have systems like the one proposed for your business. Chances are that the individual will be glad to discuss the performance of his intrusion alarm system and alert you to any problems that have been experienced with it.

Point Protection

As the name implies, point protection is used to detect the action or presence of an intruder at only a single location. This type of protection, also referred to as spot or object protection, may be employed alone in certain limited situation, but is most often used as a part of a larger system. Point protection can provide additional security for certain obvious targets, such as safes, files, vaults, jewelry counters, or other items of high value. In a sense, point protection is a backup system to insure the detection of an attempt to steal specific items should an intruder gain access to your premises without being detected. Examples of the sensors used for point protection are capacitance proximity sensors, which make metal objects such as file cabinets sensitive to the approach of an intruder, and contact vibration sensors, which detect the movement of an object.

Point protection is frequently used to protect valuable objects of art at all times, including normal business hours, and can also be used during normal business hours to protect against shoplifting. In the latter case, the alarm signal must be directed to on-site guards or security personnel, rather than to the police.

Sensors used for point protection detect the action or presence of an intruder at only one single location.

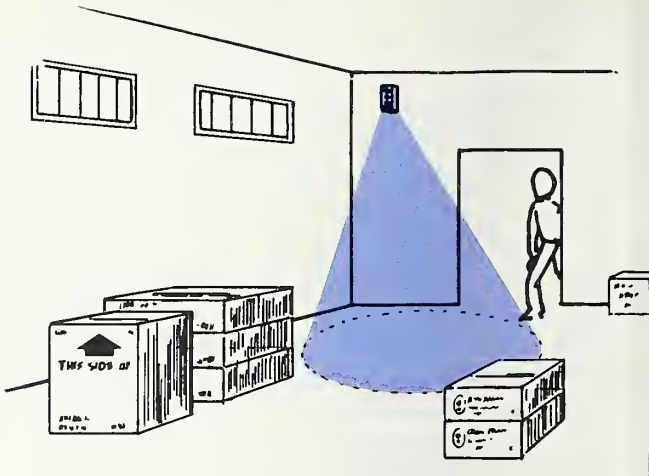
Perimeter Protection

Perimeter protection may well be the most expensive as well as one of the most practical types to install. Sensors are used to detect the action or presence of an intruder at all vulnerable building access points such as doors, windows, skylights, etc. This type of system provides early detection of an attempted or successful intrusion and increases the likelihood of apprehension. Although perimeter protection is sometimes used as the only type of protection, it is often supplemented by point or area protection. Perimeter protection generally uses switch sensors (magnetic, mechanical, or mercury) and metallic foil. The switches cause an alarm to be transmitted when the door or window is opened, and the metallic foil causes an alarm to be transmitted when it is broken.

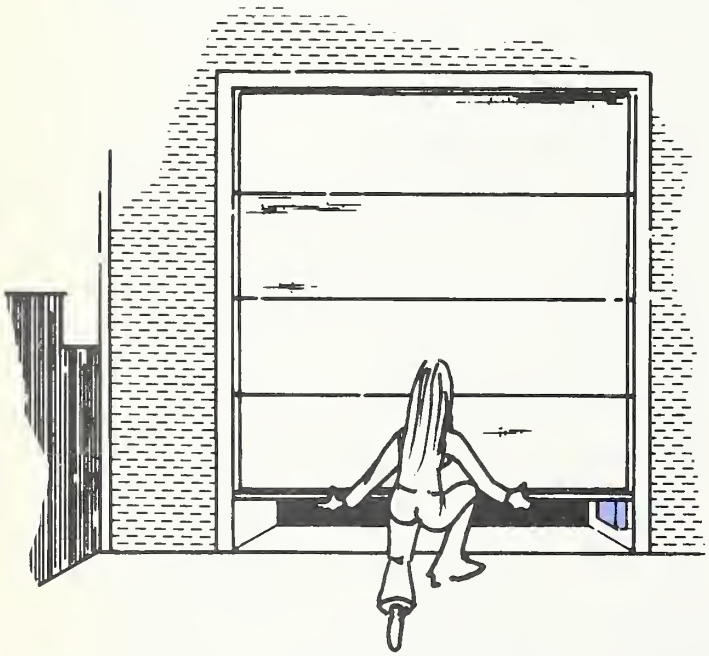
While switch sensors can be installed so as to be concealed, they are often mounted in plain view, to make it obvious that the business has an alarm system. The exposed perimeter system may serve to deter the inexperienced intruder, but it may also make it easier for the experienced burglar to counteract the sensors

and gain entry. Pressure mats, which cause an alarm when stepped on by an intruder, can be concealed under a carpet in front of doors or windows to provide perimeter protection. Such protection can also be furnished by infrared photoelectric sensors that signal an alarm when an intruder interrupts the beam.

The major disadvantage to the use of a perimeter protection system alone is that it offers no protection against persons who remain hidden inside the premises until after closing. Under these circumstances the intruder is free to burglarize or vandalize a seemingly protected establishment, signaling his presence only when he leaves the building. Obviously, the chances of apprehending the intruder are greatly reduced in this instance.



Sensors used for area protection detect the presence of an intruder within a selected area.



Sensors used for perimeter protection detect the action of an intruder at any vulnerable access point (such as a door, window, skylight, etc.).

Area Protection

Area protection, whether used alone or in conjunction with a perimeter system, is used to detect the presence of an intruder anywhere within a selected area. This type of protection is also referred to as space or volume protection because the sensors respond to intruders anywhere within their field of view. With some types of sensors, the detection zone is such that there is no entry point that can be used by the intruder without his being detected. The major consideration when using area protection alone is the choice of the proper area to be protected and the protection pattern of the sensor to be used. Area protection usually serves as a backup to perimeter protection systems by detecting the presence of the "stay-behind" burglar or the intruder who gains entry without triggering the perimeter alarm.

A variety of sensors can be used to provide area protection. Commonly employed are ultrasonic, microwave, and infrared motion sensors. The extra expense involved in using area protection in addition to perimeter protection can be justified if the value of the property to be protected is high enough, if the premises to be

protected are highly vulnerable to perimeter entry, or if the threat includes the probability of attack from hidden intruders.

Holdup Protection

A holdup alarm system is a separate circuit or subsystem of an intrusion alarm system that is active during normal working hours and consists of one or more manually actuated switches. Because the holdup alarm is actuated by an individual on the scene, judgment is required in its use.

During a holdup, you or your employees are confronted by an armed individual who is clearly a threat to life. Hence, holdup alarms are designed so that their actuation is not obvious to the robber. In this instance, the alarm signal is always transmitted to a remote location, such as a police station, with no attempt to sound an alarm at the protected premises. The armed intruder is normally in an agitated state of mind, and his reactions are difficult to predict. If he sees or suspects that an alarm has been transmitted, he could flee, or retaliate by injuring or killing any or all persons present.

Holdup devices should be selected to permit actuation with a minimum chance of detection. For example, a money clip is useful, since it permits the employee to actuate the alarm by the very action required to satisfy the demands of the robber—removing money from the cash drawer. Holdup switches should also be available at other locations, such as in a nearby office, to enable an individual outside the robber's view to actuate the alarm. If the size of your business warrants guards, security personnel, or trained individuals capable of providing assistance during a potential holdup situation, you might also consider the installation of a suspicion alarm system that an employee would actuate with an alarm button if the actions of an individual seemed to be improper. Such alarms are internal, and alert security personnel that it is necessary to observe the behavior of individuals on the premises and to be prepared to respond should an attempted robbery occur.

Holdup switches should be designed so that they cannot easily be actuated by accident. Holdup alarms receive high priority response from law enforcement personnel, who must assume that the lives of the personnel within the premises are being threatened. There is always the possibility of an accidental discharge of a firearm when an officer enters the premises prepared to defend the victims and himself.

A holdup device is a manually actuated switch set off by an employee during a holdup.

Many intrusion alarm systems that include holdup protection also incorporate surveillance cameras to record evidence for purposes of apprehension and legal action. They are usually controlled by the holdup alarm and are automatically turned on by the alarm signal. Their use in conjunction with a suspicion button is very desirable, for that permits photographs to be taken of a suspect prior to the commission of the crime. The additional precrime photographs are usually as useful as, and sometimes more useful than, those taken during the crime. The use of surveillance equipment is discussed in detail in the LESL Guide, "Selection and Application of Fixed Surveillance Cameras."

In some instances, the use of holdup switches at fixed locations is not very practical. The individual who operates a small business, perhaps as a sole proprietor, might constantly move about the premises making it difficult to provide fixed holdup switches at all possible working locations. For this reason portable holdup switches, sometimes referred to as personal panic buttons, are becoming increasingly popular. These devices are basically small radio transmitters that can be carried in a pocket and actuated in an inconspicuous manner, should the businessman be threatened. The radio signal is received by the control unit of the intrusion alarm system and an alarm signal is transmitted just as if the alarm were wired directly into the control unit.

Some businessmen also use the portable holdup switch for additional protection outside their business establishments. For example, a businessman might install a receiver on the exterior of his building, so that when he leaves after the close of business, with the proceeds for the day, he can actuate the holdup alarm if he is attacked at any point between the building and his car in the parking lot.

TABLE 1. APPLICATIONS OF INTRUSION ALARM SENSORS

SENSOR	POINT	PERIMETER	AREA
DRY CONTACT SWITCHES	⊕	●	○
MAGNETIC SWITCHES	⊕	●	○
MERCURY SWITCHES	⊕	●	○
METALLIC FOIL	⊕	●	⊕
WIRE SCREENS	●	●	⊕
TRIP WIRE	○	●	○
PRESSURE MATS	●	●	⊕
PRESSURE RIBBONS	●	●	⊕
PRESSURE WAFERS	●	○	○
ACOUSTIC SENSORS	○	○	●
ULTRASONIC MOTION SENSORS	○	○	●
MICROWAVE MOTION SENSORS	○	⊕	●
PHOTOELECTRIC SENSORS:			
PASSIVE	●	○	●
ACTIVE	○	●	○
CAPACITANCE SENSORS	●	⊕	⊕
VIBRATION SENSORS	●	⊕	⊕
INFRARED MOTION SENSORS	○	⊕	⊕

● GOOD APPLICATION
⊕ LIMITED APPLICATION
○ NOT APPLICABLE

THE SENSORS

Selecting the proper sensors for an intrusion alarm system is somewhat complicated. In most cases, it will be possible to use any of several different types of sensors for the same general type of protection. In addition to the variety of sensors available, there are literally hundreds of companies that manufacture these devices. There are differences between sensors manufactured by various companies and options to the basic designs are also offered, thus providing a wide range of choice. *Table 1* lists the sensors that are commonly used for each of the basic types of protection: point, perimeter, and area.

The sensors of an alarm system are electronic or electromagnetic devices that act as a replacement for a human observer or as a supplement to human observation. For example, when an intruder opens a door, a switch sensor can be used to detect that it has been opened—an action that would be obvious if you were watching the door. In this instance, the method of detection is extremely simple—a switch actuation. Modern technology, however, has developed sensors that use complex detection mechanisms. Sophisticated sensors are designed to "see" and signal an alarm in response to a specific stimulus or source that is considered to result from the action or presence of an intruder (movement, body temperature, footsteps, etc.). It must be remembered that sensors lack human judgment; when a sensor detects that which it is designed to detect, it will signal an alarm. Thus, motion sensors will respond to animals as though they were human intruders.

The manner in which the commonly used types of intrusion alarm sensors operate is discussed in the paragraphs that follow. Because of differences between various manufacturers' products, the comments may not be universally applicable.

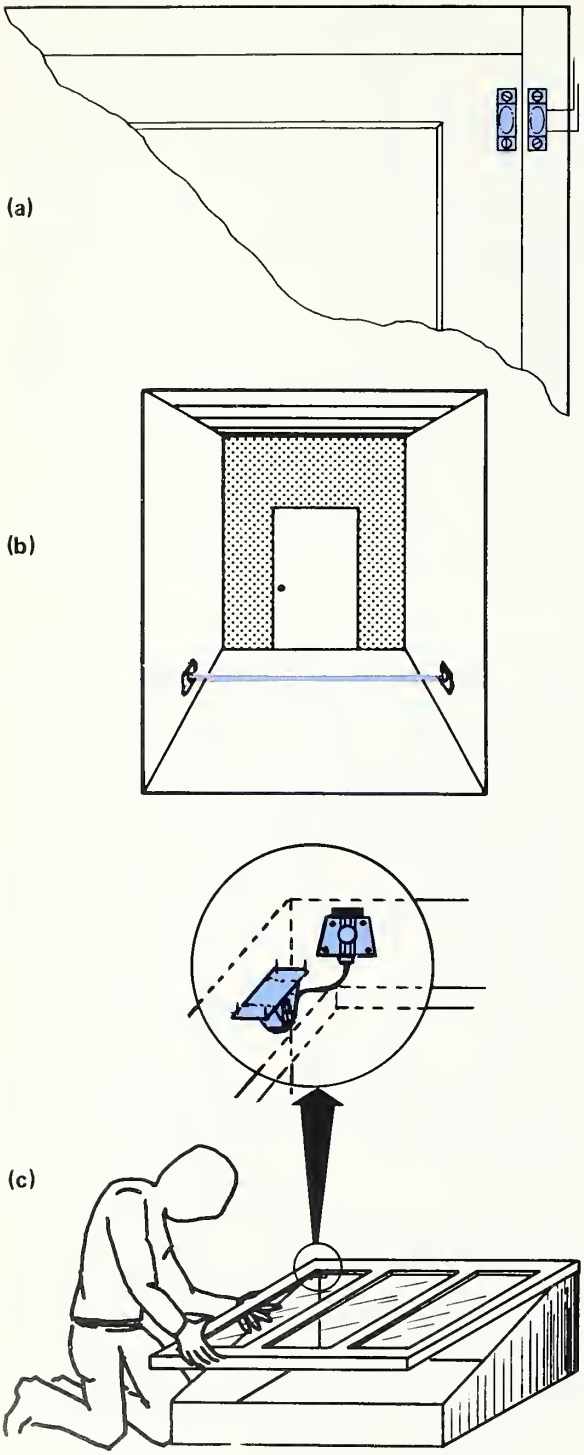
Switch Sensors

The switch sensor is undoubtedly the most frequently used intrusion alarm sensor. Switches incorporate electrical contacts that make or break an electrical circuit in response to physical movement. They are used in perimeter protection systems to detect the opening of doors and windows, and can be used as a part of a shoplifting alarm as well as in holdup alarm systems. You will find that most alarm installers refer to switch sensors as "contacts," and will often describe the proposed system as using a contact on this door, or that window, etc.

The dry contact switch is a mechanical switch similar to a light switch; several different designs are used. A plunger switch is designed to be installed in a door or window jamb, and operates like the switch that turns on the interior lights when a car door is opened. Others have small levers that are displaced by the movement of the door or window to actuate the contacts.

Nearly all switches used in holdup systems are mechanical switches. The money clip is a switch in which a bill is inserted between spring-actuated contacts. When the teller takes the bill from the switch, the contacts close and the alarm is sent. It is also possible that the thief himself can unwittingly sound the alarm, for the money clip is hidden below a stack of bills. The switches that an individual can actuate in case of a holdup include a foot rail, which is operated by placing one's foot under a rail and applying pressure with the toes in an upward manner, and hand operated switches. Those intended for hand actuation should incorporate two buttons that must be pushed simultaneously. All holdup switches should be designed to make accidental actuation difficult.

A trip switch is a mechanical switch designed so that the contacts close when a small plug is removed from the body of the switch. In one application the switch is positioned on a wall, perhaps in a corridor, slightly above the floor. A thin wire is attached to the switch plug and stretched to a fixed point on the opposite wall. If an intruder walks into the wire, the plug is pulled out and the alarm is sounded. Trip switches are also used on overhead doors, such as garage doors.



Switch sensors have electrical contacts that make or break an electrical circuit in response to a physical movement; they are usually used for perimeter protection. This illustration shows three types of switch sensors: (a) magnetic switch, (b) trip switch, and (c) mercury switch.

Intrusion alarm systems often use magnetic switch sensors. Like any electrical switch, magnetic switches can be obtained with either normally open or normally closed contacts. Most intrusion alarm systems use the normally closed type of switch regardless of whether it is mechanically or magnetically actuated.

The magnetic switch consists of two components, each contained in a separate housing. The switch is a pair of contacts that will open or close when subjected to a magnetic field. A separate magnet is mounted near the switch to set the contacts to the normal position. The magnet is mounted on the moveable member of the item that is being protected, such as a door or a window sash. When it moves away from the switch the contacts are actuated.

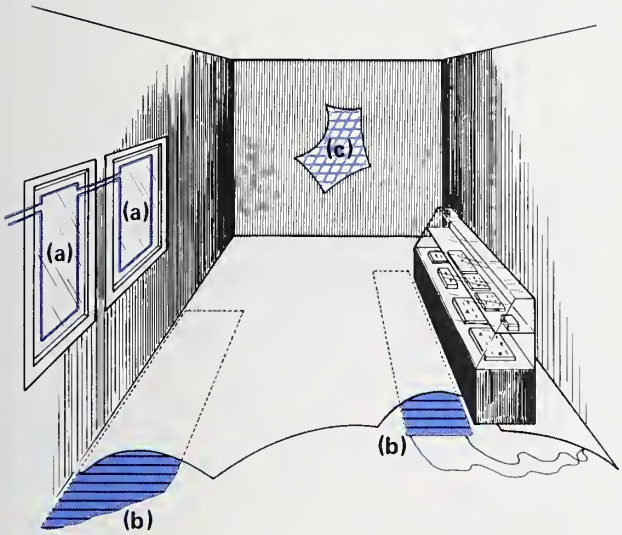
Since the switch contacts are held in their normal position by a magnetic field, it is possible to place a strong magnet near the switch and thus prevent the contacts from actuating when the switch magnet is moved away. For this reason, a second type of magnetic switch, the balanced magnetic switch, has been developed. This employs two magnets with fields that interact to produce a net field surrounding the switch contacts. The balance of this net field is so critical that if it is disturbed by placing a non-system magnet near the switch, the contacts will be actuated to signal an alarm.

Mercury switches, which the installer might call "tilt switches," are used, as an example, to detect the movement of a transom. The mercury switch consists of contacts within a sealed unit containing a small pool of mercury. When the switch is tilted, or pivoted in a vertical plane, the mercury rolls between or away from the contacts to either complete or open an electrical circuit.

Pressure Mats

Pressure mat switches are basically mechanical switches. You have probably encountered them in your local grocery or department store, where they are frequently used to automatically open the doors as you approach. In intrusion alarms,

the pressure mat is most frequently used as a backup system, e.g., to detect an individual stepping on the floor below a window through which entry has been gained without causing the perimeter system to alarm. Pressure mat switches are also used as "traps" because they can be hidden under the carpet in front of a likely target such as a valuable appliance, on stairs, and in corridors which one would expect an intruder to use.



Metallic foil (a) breaks when the glass is broken; this triggers an alarm. Pressure mats (b) respond to pressure; they cause an alarm when stepped upon. Concealed wire screens or grids (c) respond to forced entry through walls, ceilings, doors, etc.

Miniature pressure mat switches are also available for use in shoplifting alarm circuits. These switches are placed under objects of value and will cause an alarm if the protected item is picked up.

Pressure mats are versatile sensors. Although normally designed to actuate in response to a weight of 7 kg (15 pounds) it is possible to obtain them with either higher or lower sensitivity. They are made in a large variety of sizes, ranging from approximately 1 centimeter (less than 1/2 inch) to over a meter (several feet) in width, and in almost any length you might desire.

Metallic Foil

Metallic foil, one of the simplest intrusion alarm sensors, is commonly attached to glass to detect breakage. When the glass is broken the foil also breaks and an alarm is signaled. While metallic foil is most often used on display windows, it is also used in doors with glass glazing and on display cases containing valuable merchandise.

Metallic foil can be easily damaged by routine housekeeping activities such as cleaning. Therefore, it is normally covered with a thin coat of shellac or varnish after it has been attached to the glass surface with adhesive.

Wire Screens

Wire screens or grids are sometimes used in intrusion alarm systems. This is a closely spaced pattern of thin electrical wires, usually forming a grid pattern 10 to 15 centimeters (4 to 6 inches) square. Such a grid can be used to detect forced entry through walls, ceiling, doors, etc. The wire can also be incorporated into the mesh of a normal window screen. When a wire is broken an alarm is sounded, just as with metallic foil on a window.

When a wire screen or grid is used, it is most often covered with wallpaper, building material, or some other material, both to conceal it and to protect it from being broken by normal housekeeping.

Microwave Motion Detectors

Microwave motion detectors are used to sense the presence of an intruder within a volume of space or an area. These devices transmit a high frequency electric field that is monitored by a receiving antenna. The frequency of the electric field changes when reflected from a moving object, and an electronic processor circuit compares the transmitted frequency with that which is received, signaling an alarm when a change in frequency is detected.

TABLE 2. COMPARI

SENSOR	DRY CONTACT MECHANICAL SWITCHES	MAGNETIC SWITCHES	MERCURY SWITCHES	METALLIC FOIL	WIRE SCREENS	TRIP WIRES	PRESSURE PRESSURE R PRESSURE
APPLICATIONS	DOORS, WINDOWS, GATES, TRANSOMS, HATCHES, ETC., USUALLY FOR PERIMETER PROTECTION.	DOORS, WINDOWS, GATES, TRANSOMS, HATCHES, ETC., USUALLY FOR PERIMETER PROTECTION.		SHOW WINOOWS, OFFICE WINOOWS, GLASS DOORS, DRY WALL BOARD, ETC., USUALLY FOR PERIMETER PRO-TECTION.	ACCESS POINTS NOT SUBJECT TO EVERY-DAY USE, USUALLY FOR PERIMETER PROTECTION	ENTRY WAYS SUCH AS TO CORRIDORS OR IN OOORWAYS FOR PERIMETER PROTECTION.	SMALL AREAS DOORWAYS, UNDER SPEC OBJECTS FOR POINT PROTE
ADVANTAGES	LOW COST.	RELATIVELY RESISTANT TO ENVIRONMENTAL EF-FECTS. RELATIVELY IMMUNE TO EFFECTS OF WEAR. LOW COST.	(SAME COMMENTS AS FOR MAGNETIC SWITCHES APPLY; APPLICATION IS USUALLY FOR ACCESS POINTS THAT HAVE COVERS THAT OPEN WITH CHANGING VERTICAL ANGLE. THUS THESE SWITCHES OPERATE WHEN TILTED BEYOND A CERTAIN POINT.)	EASILY REPAIREO. VISIBILITY SERVES AS DETERRENT.	LOW DEGREE OF MAINTENANCE. LOW VISIBILTIY FOR ATTRACTIVE APPEARANCE.	LOW COST.	LOW COST, LOW OEGREE MAINTENAN ADAPTABLE TO VARIETY OF ANO SIZES.
DISADVANTAGES	LOW RELIABILITY LOW SENSITIVITY. SUBJECT TO ENVIRON-MENTAL EFFECTS. HIGH INSTALLATION COST.	BECAUSE OF MOUNTING POSITION, MAY BE SUBJECT TO DAMAGE IN SOME APPLICATIONS. HIGH INSTALLATION COST.		VULNERABLE TO DAMAGE BOTH IN-TENTIONAL AND THROUGH DAY-TO-DAY USE.	MUST BE REPLACED AFTER PENETRATION TO RESTORE PROTECTION.	MUST BE REMOVED TO ALLOW NORMAL ACCESS, THEN REPLACED TO RESTORE PROTECTION.	SUBJECT TO IN PATH OF TRAFFIC. SUBJECT TO OF HUMIDIT STANDING W
RESISTANCE TO DEFEAT	LOW.	BALANCED TYPE MORE RESISTANT TO COMPROMISE THAN SINGLE MAGNET TYPES.		LOW.	MOOERATE FOR CON-CEALED TYPES.	LOW IF DETECTEO BY INTRUOER.	RELATIVELY ONLY IF CC OR PRESEN KNOWN TO
FALSE ALARM SUSCEPTIBILITY	HIGH IF OOOR OR WINDOW HAS LARGE AMOUNT OF PLAY; LOW IF TIGHT.	HIGH IF DOOR OR WINDOW HAS LARGE AMOUNT OF PLAY; LOW IF TIGHT.		HIGH DUE TO EFFECTS OF ENVIRONMENT.	LOW TO MODERATE.	LOW IF BUILDING IS SOLID.	SUBJECT TO MENTAL CO

INTRUSION SENSORS

ACOUSTIC SENSORS	ULTRASONIC MOTION SENSORS	MICROWAVE MOTION SENSORS	INFRARED MOTION SENSORS	PHOTOELECTRIC (ACTIVE) SENSORS	PHOTOELECTRIC (PASSIVE) SENSORS	CAPACITANCE SENSORS	VIBRATION SENSORS
EA PRDTECTION F ENCLDSED ACES (ROOMS, AULTS, ETC.).	AREA PRDTECTIDN OF SMALL EN-CLDSED SPACES (RDDMS, CDR-RIDDRS, ETC.)	AREA PRDTECTIDN OF ENCLDSED SPACES (ROOMS, CORRIOORS, ETC.) CAN COVER LARGE AREAS.	AREA PROTECTION OF ENCLOSED SPACES (ROOMS, CORRIODRS, ETC.) CAN COVER LARGE AREAS.	ACRDSS OOORWAYS, CORRIOORS,ETC., FOR PERIMETER PROTECTIDN; MULTIPLE BEAM SYSTEMS FOR LIMITED AREA PROTECTIDN.	POINT PROTECTIDN USING SENSORS WITH HIGH DIRECTIDN SEN-SITIVITY; LIMITED AREA PRO-TECTION OF SMALL ROOMS OR PORTIDNS OF LARGER ONES.	PRIMARILY POINT PROTECTION FOR SAFES, FILING CABINETS, VALUABLE OBJECTS, LIMITED AREA AND PERIMETER PRDTECTION.	PRIMARILY POINT PRDTECTIDN FOR VAULTS, SHOW-CASES, ETC.; LIMITED SPACE PROTECTION WHEN INSTALLED TO PROTECT WALLS OR CEILINGS, ETC.
ISITIVE. USE EXIST-G INTERCOM STEMS. T AFFECTED BY R MOVEMENT. ECTIVE AGAINST TAY-BEHINDS."	USUALLY NOT DETECTABLE BY INTRUDER. EFFECTIVE AGAINST "STAY-BEHINDS." EASY PHYSICAL INSTALLATION.	NDT DETECTABLE BY INTRUDER. EFFECTIVE AGAINST "STAY-BEHINDS." NOT AFFECTED BY AIR MOTION, NOISE, LIGHT DR SOUND.	RELATIVELY IMMUNE TO NOISE AND VIBRATIDN.	HIGH DEGREE OF FLEXIBILITY IN APPLICATION. INFRARED BEAM DIFFICULT TD DETECT. CAN COVER ACCESS POINTS WHERE PHYSICAL OB-STRUCTION NDT DESIRED OR CAN-NOT BE TOLERATED.	RELATIVELY UN-AFFECTED BY ENVIRONMENTAL FACTORS (EXCEPT ABRUPT CHANGE IN LIGHT LEVEL). HIGH DEGREE OF FLEXIBILITY IN APPLICATION.	HIGH DEGREE OF FLEXIBILITY IN APPLICATIDN. PROTECTIVE FIELD NOT DETECTABLE BY INTRUDER.	REDUIRE LOW MAIN-TENANCE. HIGH DEGREE OF RELIABILITY WHEN PROPERLY APPLIED.
ST BE USED IN ABLE NOISE VIRONMENT ERE BACKGROUND VEL IS LOW.	SEVERELY AFFECTED BY ENVIRDNMENTAL FACTDRS; AIR TURBULENCE AND MOTION, RATTLING DOORS, JANGLING KEYS, BLOWING DRAPERIES, VIBRATIONS, LOUD NOISES, ETC. ESSENTIALLY LINE-OF-SIGHT OPERATION; LARGE OBJECTS COULD SHIELD INTRUDER. MAY NOT DETECT EX-TREME RATES OF MOVEMENT (VERY SLOW OR VERY FAST).	CDVERAGE DIFFICULT TD CONFINE TO DE-SIRED AREA. CAN BE SET OFF BY NEARBY FLUORES-CENT LIGHTS, LARGE OBJECTS OUTSIDE PROTECTED AREA, RADIO TRANSMITTER OPERATING NEAR SENSOR FREQUENCY.	SOME SYSTEMS SENSITIVE TO CHANGES IN THERMAL ENVIRON-MENT (e. g., CHANGES IN SUNLIGHT AND TEMPERATURE).	NARROW BEAM OF PRDTECTION. LINE-OF-SIGHT OPERATION; SMOKE OR DUST CAN HAMPER OPERATION. SUBJECT TO MIS-ALIGNMENT PROBLEMS.	NARROW BEAM OF PROTECTION. LINE-OF-SIGHT OPERA-TION; SMOKE OR DUST CAN HAMPER OPERA-TION.	CAN BE APPLIED ONLY TO OBJECTS NOT ELECTRICALLY GROUNDED; MAY REQUIRE SPECIAL CONSTRUCTION.	DETECTS ONLY FORCE-FUL ATTEMPTS AT ENTRY. CANNOT BE USED IN AREAS OF HIGH VIBRATION (TRAFFIC, CONSTRUCTION, ETC.)
H IF PROPERLY TALLED.	HIGH IF PROPERLY INSTALLED.	HIGH IF PROPERLY INSTALLED.	HIGH	LOW TO MODERATE, WITH SYSTEMS USING MODULATED BEAMS HAVING HIGHEST RESISTANCE.	HIGH	VERY HIGH.	VERY HIGH.
BE HIGH BUT DUCED USING DITIONAL CAN-LATION MICRO-NE.	CAN BE HIGH UNLESS ENVIRONMENTAL FACTORS ARE CON-SIDERED BEFORE APPLICATION.	CAN BE HIGH UNLESS PROPERLY PLACED AND CAREFULLY ADJUSTED.	HIGH FOR RECEIVE-ONLY SENSORS. LOW FOR TRANSMIT-RECEIVE SENSORS.	CAN BE HIGH IF CERTAIN ENVIRON-MENT FACTORS ARE PRESENT (SMOKE, DUST) OR POOR PLANNING RESULTS IN MISAPPLICATION.	CAN BE HIGH IF IMPROPERLY INSTALLED SO THAT HEAT OR LIGHT LEVELS ARE NOT CONSTANT; IF COVERS FLOOR, RODENTS MAY SET OFF ALARM.	LOW IF PROPERLY INSTALLED.	CAN BE HIGH IF ENVIRONMENTAL FACTORS ARE NOT TAKEN INTO AC-COUNT; MAY BE TRIGGERED BY MINOR EARTH TREMORS, SONIC BOOMS OR TRAINS.

The microwave field can be generated in all directions, just as light from a bare light bulb is radiated in all directions, or it can be transmitted in a controlled pattern similar to the focused light beam from a flashlight. Many manufacturers offer a variety of transmitting antennas to enable the user to select a field pattern that best suits his needs.

Bistatic microwave motion detectors utilize separate transmitting and receiving antennas mounted at opposite ends of the space or area to be protected. Monostatic units have the transmitting and receiving antennas mounted in the same unit, sometimes using a single antenna to both transmit and receive the microwave signal. The detection range of a microwave motion sensor is dependent upon the electrical power of the transmitted field, the shape of the field, and the operating frequency. The most commonly used frequencies are between 915 and 10,525 megahertz.

Microwave energy will penetrate and pass through nearly all building construction material (wood, sheetrock, cinder block, plastic, glass and brick) and is reflected from metal. The amount of penetration increases as the microwave frequency decreases. Since the field from a microwave motion sensor will penetrate walls, proper application is important. If the field is not contained within the desired area or space, the microwave motion detector can respond to motion in adjoining rooms, or to motion outside the building. On the other hand, metal surfaces or structural steel within walls and floors will reflect the microwave energy and can distort the shape of the field so that the detector will respond to motion in areas not expected to be included within the field.

The manufacturer's equipment specifications will normally include sketches of the microwave field shape for each antenna. The actual field of an individual unit will vary somewhat from that indicated in the manufacturer's literature. Each antenna will, for the most part, have its own unique transmission characteristics as a result of normal manufacturing variation. Detection ranges of several hundred feet are not uncommon for microwave motion detectors, and these are frequently used in outdoor installations.

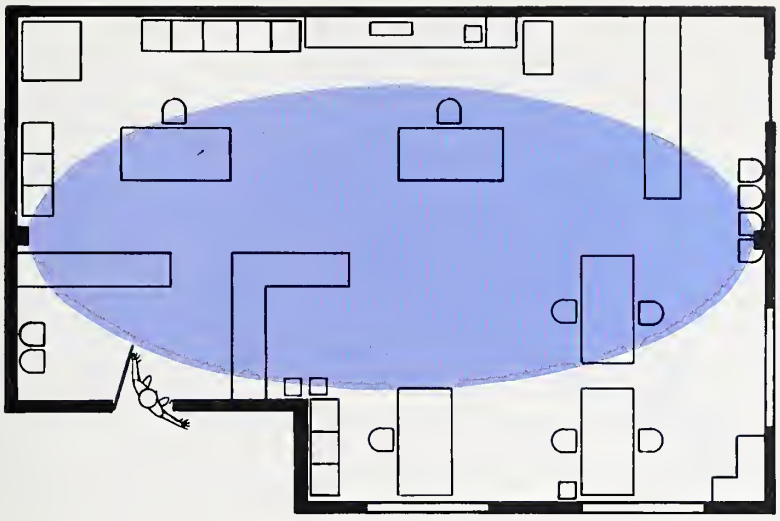
Although various manufacturers incorporate different processing circuitry into microwave motion detectors, practically all systems accomplish detection on the basis of frequency shift. The basic logic of the alarm circuit can use different criteria to interpret what signal will be judged to constitute an alarm. There will be differences in the amount of frequency change or the value of the integration time constant (the minimum period of time that the frequency change must be present) before an alarm is signaled. Some equipment is designed so that a specific sequence of signal events must occur before it will signal an alarm.

Ultrasonic Motion Detectors

Ultrasonic motion detectors operate on the same principle as microwave motion detectors, namely sensing the presence of an intruder through the effect of his motion upon a field within a volume of space. In this instance, however, the field is ultrasonic energy (high frequency sound) rather than an electrical field. Most ultrasonic motion sensors generate signals in the range between 19 and 40 kilohertz, which is above the frequencies that the average human can hear. Movement within the field of ultrasonic energy generated by the unit causes the frequency of the reflected signal to change.

Ultrasonic motion detectors use a transmitting element to generate the ultrasonic energy, a receiving element to monitor the frequency of the signal, and an electronic processing circuit that compares the transmitted and received signals. As with microwave motion detectors, a variety of signal processing techniques are used by the various manufacturers.

Monostatic ultrasonic motion detectors enclose the transmitting and receiving elements in a single unit, and are used to protect a space of perhaps 6 by 9 meters (20 by 30 feet) in a room with a ceiling up to about 3.5 meters (12 feet). These units are normally mounted on a wall or at a ceiling corner. Bistatic ultrasonic motion detectors employ separate transmitting and receiving elements. Often, both elements are located remotely from the processor, and the system can be designed to use multiple



Microwave and ultrasonic motion detectors sense an intruder's motion through their energy fields. The microwave motion detector transmits a high frequency electromagnetic field; the ultrasonic motion detector transmits a high frequency sound field.

receiving elements with a single transmitting element. A typical installation would include a single transmitting element mounted in the ceiling near the center of the room, with two or more receiving elements, also mounted in the ceiling, around the transmitting element. In some cases, bistatic units are designed to allow the use of both multiple transmitting and receiving elements.

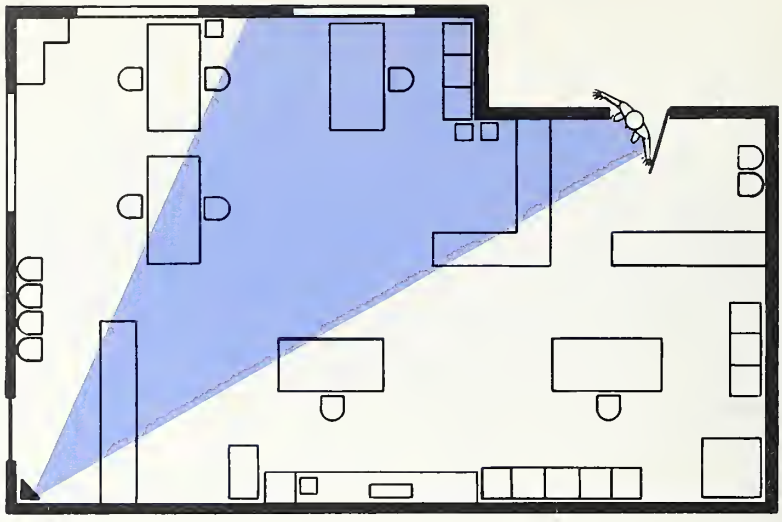
Ultrasonic energy can be completely contained within a room, for it will not penetrate most structural materials, and it is, like any sound energy, absorbed by carpet, draperies, and acoustical tile. Obstructions within a room will reflect the ultrasonic energy, and will distort the shape pattern of the transmitted energy. In addition, merchandise display cases, tables, or cabinets can block the ultrasonic signal, and create blank spots. The detector will not respond to motion within such areas. Keep this in mind if you use ultrasonic motion sensors in large warehouses, for if the size and location of stock piles of merchandise change often, the detection zone of the sensor may also be changed.

Infrared Motion Detectors

Infrared motion detectors are passive sensors, because they do not transmit a signal for an intruder to disturb. Rather, a source of moving infrared radiation is detected against the normal radiation environment of the room. These detectors are designed to sense the radiation from a human body moving through the optical field of view.

Infrared motion detectors are normally sensitive enough to sense the moving radiation from a human at distances of 9 meters (30 feet) or more. Temperature changes of the room or stationary items within the room do not cause the infrared motion detector to sound an alarm. Since these devices rely upon the differences in radiation between the room and an intruder, use in a room that is maintained at a temperature approaching that of a human body could limit the effectiveness of the device.

Infrared motion detectors use an optical system to project an image of the area, within their field of view, onto a radiation sensor. Some of these detectors employ a very narrow field of view and are useful for point protection, to monitor a long narrow corridor, or to provide line protection. Those designed to provide a wide field of view utilize either continuous area coverage or multiple zone coverage. In the first type, the detector will sense a moving source of radiation anywhere within the image that is formed on the radiation sensor. In the case of the zone type detector, the radiation sensing element consists



Infrared motion detectors are passive; they do not transmit a signal. Instead they detect a source of moving infrared radiation—the intruder—against the normal radiation environment of the room.

of many individual sensors, each located at a specific point within the radiation image so as to sense moving radiation from a small area or volume within the total field of view. When using a zone type detector, alignment is critical. Wide angle infrared motion detectors normally have a field of view in excess of 90 degrees, and when mounted in a ceiling corner can provide good coverage of a 9 by 9 meter (30 by 30 foot) room. Infrared motion detectors with much wider fields of view are available for use as wall-mounted installations.

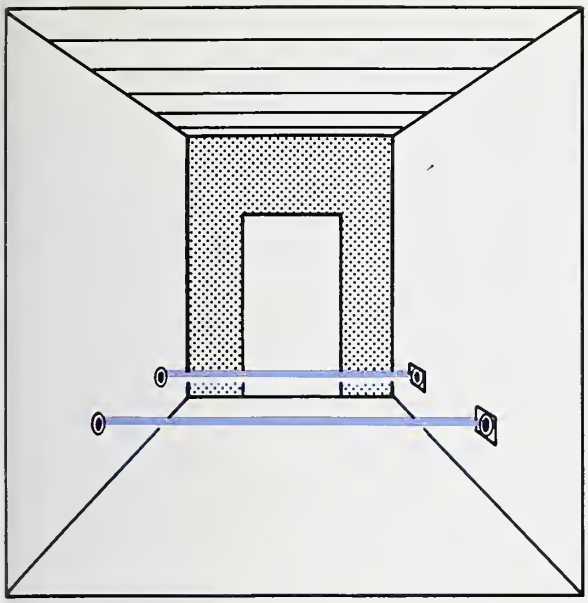
Infrared Photoelectric Sensors

Infrared photoelectric sensors are another type of optical sensor. A narrow beam of invisible infrared light is directed across a corridor, along a wall, or across a path that one would expect an intruder to travel. A receiver monitors the beam, and signals an alarm if the beam is interrupted. The earliest photoelectric sensors used visible light, and are now often used to open the doors of grocery and department stores.

Visible light, for obvious reasons, is not suitable for use with photoelectric sensors for intrusion alarm systems. Infrared photoelectric sensors use infrared laser sources or white light sources and infrared filters. Many of the available sensors utilize high energy sources that are capable of transmitting a beam over distances of more than 100 meters (more than 300 feet) and are most commonly used in outdoor systems.

Frequently, the sensor's transmitter or light source and receiver are separate units; many, however, mount the source and receiver in the same housing. These systems, called retroreflection systems, require the use of a mirror to return the beam to the receiver. Mirrors can be used with either type of infrared photoelectric sensor to direct the protective beam around the entire perimeter of an area or along almost any desired optical path.

Because the receiver is so designed that it will not signal an alarm as long as it is exposed to infrared radiation, it would be a simple matter to shine infrared radiation from a flashlight or other light source into the receiver optics and thereby defeat the system. Most infrared photoelectric sensors prevent such action by modulating the light source. The light beam is transmitted as a series of pulses rather than as continuous radiation. The electronic circuit of the receiver is designed to signal an alarm if the received radiation is not properly modulated.



A narrow beam of invisible infrared light, monitored by a receiver, is directed across the expected path of an intruder. If the beam is broken, the monitor signals an alarm.

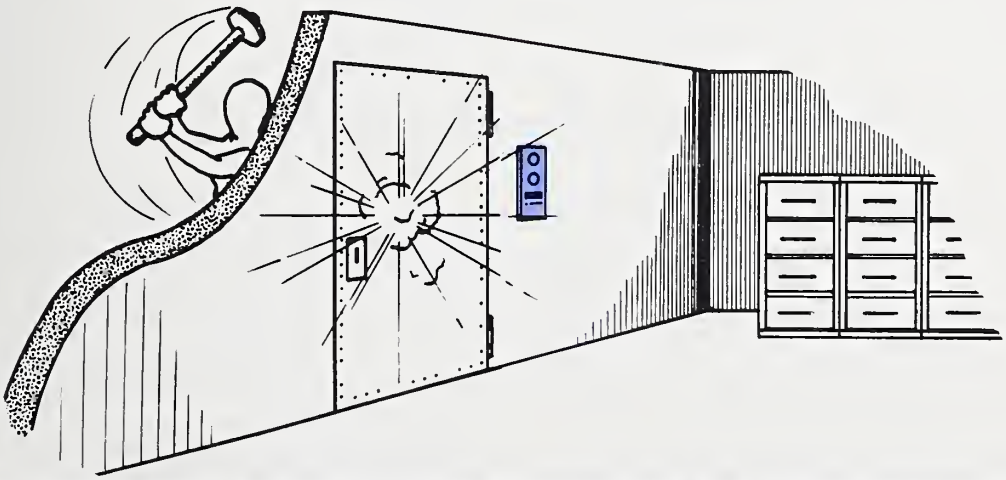
Sound Sensors

Sound sensors detect intrusion by detecting the noise created by the implements used during an attempt to break into a protected area or the sounds produced by the intruder. These devices consist of a microphone and an electronic processor. When the sound level increases beyond the limit normally encountered in the area, the unit signals an alarm. Sound sensors are most often used to protect vaults.

Sound sensors respond to continuous noise, such as that produced by drilling or sawing through a structure, but can also employ integration or pulse counting circuits. Pulse counting is used to detect noise from implements such as hammers, which do not produce a continuous sound. The integration feature examines the noise detected by the microphone over a short time interval, and an alarm is signaled if the total energy accumulated from all noise exceeds a preset level. Thus, the noise from a single large pulse, such as that from an explosion, will also cause the sound sensor to signal an alarm.

In some instances, a sound sensor may be used in an area that contains a source of audible noise, such as a compressor or a fan motor. Because such equipment only operates intermittently, it is difficult to adjust the threshold sound level to allow proper response to intrusion noises. For such applications, sound sensing units are available that permit the use of a cancel-microphone in addition to the one used to detect attack noises. The cancel-microphone is placed close to the source of intermittent sound, and the processing unit subtracts the cancel-microphone signal from that of the intrusion sound sensing microphone.

Also available are sound sensor units that enable a guard to listen directly to the sounds within the protected area by playing the microphone signal through a conventional radio speaker.



Sound and vibration sensors detect either the noise or vibrations made by an intruder attempting a forced entry into a protected area.

Vibration Sensors

Vibration sensors are used to detect the presence of an intruder by monitoring the vibrations produced when attack tools are used to penetrate the structure members (such as walls or floors) of a building.

The simplest of the vibration sensors is a mechanical switch designed so that the contacts vibrate with the surface on which they are mounted. When the vibration level exceeds a preset level, the contacts signal an alarm.

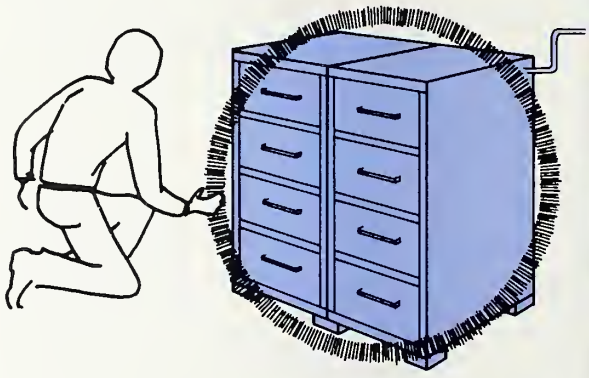
Contact microphone vibration sensors are used for the same purpose. The microphone vibration sensor is an electromechanical device that produces an electrical signal proportional to its physical displacement. These devices operate on a principle similar to that of a phonograph pickup and are used with a processor that is like the processor used in a sound sensor. In fact, some sound sensing devices are designed to accept signals from both sound sensing microphones and contact vibration microphones.

Capacitance Sensors

Capacitance sensors monitor the capacitance (capacity for the storage of electrical energy) between specific metal objects and the electrical ground of the earth. Any metal object that is electrically insulated from the electrical ground of the earth will have a capacitance associated with it. The capacitance sensor is connected to the metal object, such as a filing cabinet or a safe. The electrical field surrounding the protected object is disturbed when an intruder enters the field, causing the overall capacitance to change. The sensor signals an alarm in response to the change in capacitance.

The electronic processing circuitry of the sensor can be adjusted to respond both to the total capacitance change and the rate of change of the capacitance of the protected object. These devices can be used to protect one or more objects, depending upon the design of the sensing circuit.

Capacitance sensors can be used with grid wires or screens to protect an area such as a wall or a window; however, such use is not frequently encountered.



A capacitance sensor detects a change in the electrical field surrounding an object when an intruder enters that field. This change causes the alarm to go off.

SYSTEM DESIGN CONSIDERATIONS

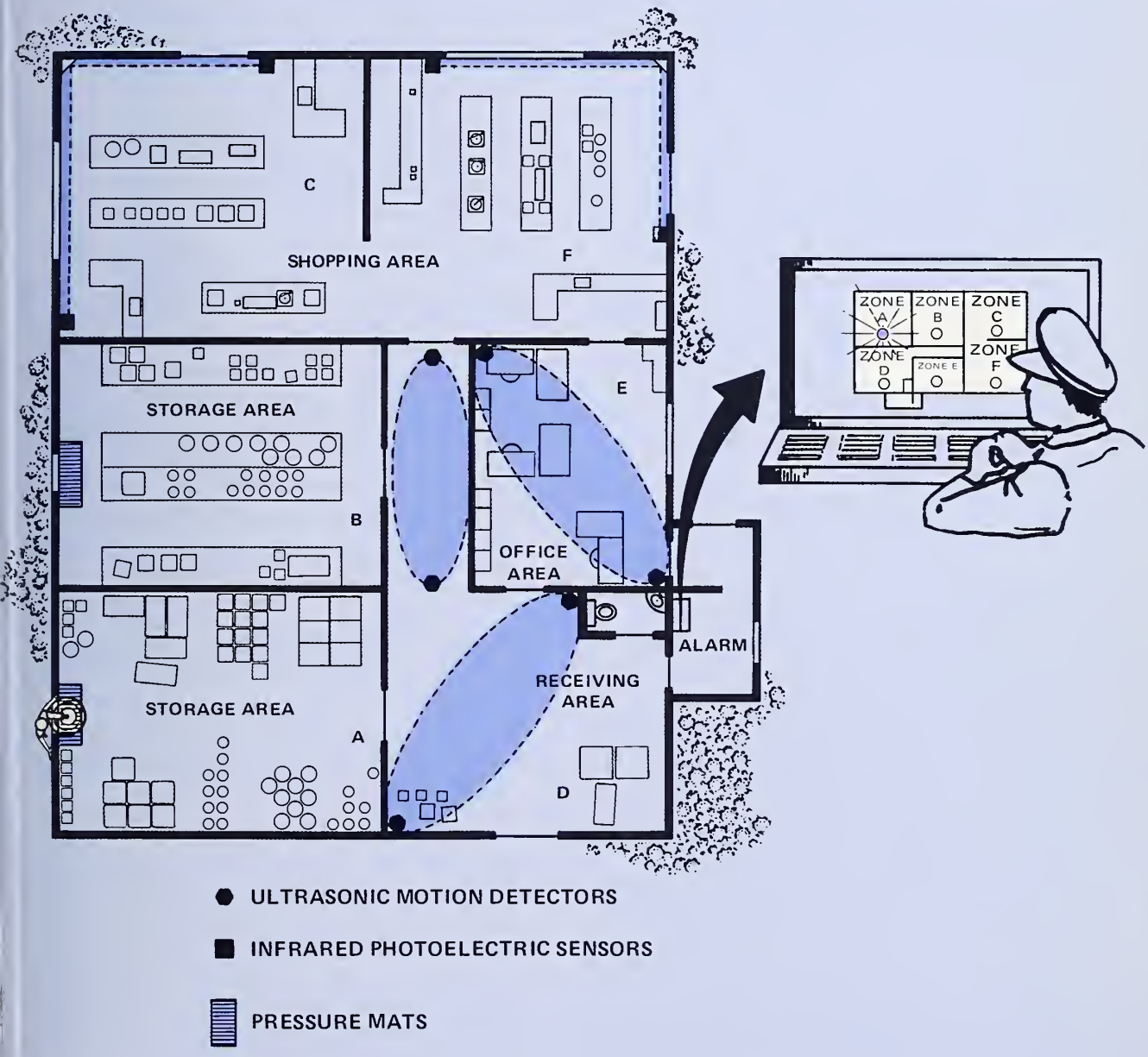
The nature and location of your business will have an important bearing on the design of an appropriate alarm system, for these factors will in general dictate the perimeter and interior protection that is needed. The design of a system that achieves the desired degree of protection depends largely on the layout of your facilities and your routine operating procedures.

The floor plan of your business is the basic consideration in the selection and location of the required sensors. Your business practices are the basic consideration in the design of the operating modes of the alarm system, which in turn will dictate the selection of the control unit. All of the above factors must be considered in order to determine the need for tamper protection. The basic system design will, of course, also depend on the manner in which the alarm signal is to be transmitted—a topic of separate discussion.

The Floor Plan

When you analyze the threat to your business and consider the alternative types of protection, you will find that a floor plan of your premises is a valuable aid. The floor plan should note all doors and windows, room sizes, skylights, interior doors to basements, and the location of high value items.

You can quickly trace the likely routes of an intruder and identify the locations that you might wish to protect with point or volume sensors. You should also consider the types of equipment or sources of false alarm stimuli at various locations within the premises. Similarly, you should also study the various locations to determine which areas are routinely available to the general public or customers during normal



A floor plan of your business will help you determine if it is necessary to divide your store into zones of protection. This type of protection not only lets you know an intruder is on the premises of your business, it also tells you which zone he is in.

working hours. This last factor will help you to determine the need to protect the sensors or other alarm components from being tampered with by an individual planning a return to your business after normal working hours.

The floor plan is also very useful when you compare proposals from each of the several alarm installers that you have asked to provide quotations. Marking a copy of the floor plan to show each sensor and its location as proposed by each bidder can help you quickly isolate the basic differences among the proposed systems. When the basic differences have been determined, you should ask each bidder to explain his choice in detail. It could be that he has recognized a need that you or the other installers have failed to consider, or he might be basing his selection upon experience and/or a specific product line that he routinely sells.

In most cases, the tradeoffs proposed by each alarm installer will be obvious. One installer might choose to protect display windows with only metallic foil, while another might prefer to use a pressure mat along the floor below the window, or perhaps use an ultrasonic motion sensor to protect the entire portion of the building behind the window and the door. When you review the proposal, you should include on the floor plan the protection volume or envelope of the sensor.

The floor plan will serve an additional purpose—it will help you to determine whether it is appropriate to separate the system into zones of protection. For example, if your facility includes a warehouse that is infrequently visited during the normal working day, you might choose to keep that part of the alarm system active during normal working hours although the rest of the system is turned off. Similarly, if you include a system to protect against shoplifting, this would be a separate circuit, or zone. In the case of a larger business that covers a large floor area, such as a major department store, it is desirable to incorporate multiple zones so that the police or guards who respond to an alarm can go directly to the area where the intruder has been detected.

If you operate a small business located in a typical suburban neighborhood shopping center, characterized by the glass front and dropped acoustical tile ceiling, take a good look at the space above the ceiling tile. You will probably find that there is no barrier between your space and that of the adjoining businesses. If this is the case, you are vulnerable to an intruder who enters a business at one end of the row, climbs into the overhead space, and travels to any store in the complex. Perimeter protection alone is inadequate under such conditions.

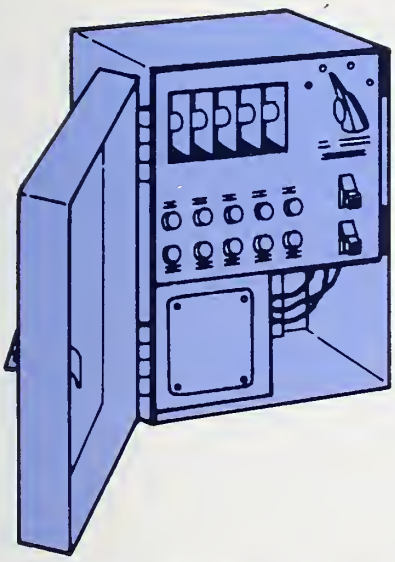
Control Units

Individual intrusion alarm sensors are usually connected to a master control unit that receives their signals and causes a local alarm to sound or alerts the police or the central station to the fact that your system has entered the alarm state.

Unless you have selected a system that does the job by low-power radio, it will be necessary to connect the sensors to the control unit with electrical wire. In that case, you will have to choose between visible wiring that is strung along the walls next to molding or completely concealed wiring, which is considerably more expensive to install.

The type of control unit that you select will depend upon the sophistication of your overall intrusion alarm system. In some cases, the control unit can be a part of one of the components. For example, if you determined that a single ultrasonic motion detector with a local alarm would adequately protect your business, without the need to install perimeter protection, the ultrasonic unit would provide relay contacts that would turn the local alarm on and off.

More complex alarm systems, however, will have a separate master control unit. This unit will provide separate input circuits for each alarm zone that you wish to incorporate into your system, and it will also provide the electrical current that flows through the switch sensors. It may also be used to provide the electrical power for the other sensors.



Individual intrusion alarm sensors are usually connected to a master control unit that receives their signals and sets off a local or remote alarm.

The control unit is the source of backup or standby power for at least the switch sensors. Should your neighborhood have a complete electrical power failure, the intrusion alarm would be inoperative without standby power. Standby power requirements, to insure protection during a power failure, are the subject of debate and depend upon the nature of the business. Installers recommend a 4 to 12-hour capability of operating from standby power. However, financial institutions are required to have a 72-hour capability of operating from standby power.

Batteries are used universally for standby power. Some equipment uses conventional dry cells, which must be replaced when their shelf-life is at an end. Other equipment uses rechargeable batteries. In some equipment, the batteries are wired to a low-power charging unit, called a trickle charger, which maintains the batteries in a fully charged condition as long as the system is connected to electrical power. If the equipment does not include a charger, the batteries must be periodically checked and fully recharged when necessary.

If the control unit or a sensor contains an integral battery charging circuit, you should determine the power capacity of the charging circuit. If the charger cannot operate the sensor and simultaneously recharge the battery, you could have a problem. Some of the equipment that has been tested did not have sufficient power capacity. In those cases, when the line power was restored after a power failure, all of the power went into charging the battery and the detector provided either greatly reduced or no protection until the battery had been recharged.

The control unit will normally incorporate a key-operated selection switch that you use to place it into the appropriate mode of operation. This may have only two positions (on and off) or it may also include a test position. The test position places all of the sensors in operation and allows you to test each component of the system without sounding a local alarm or transmitting a signal to the police or central station. Since your system will require periodic maintenance and checking, make certain that you have this test capability. Control boxes that are used for both intrusion detection and holdup protection will have still another selection position. In this case it will probably be labeled off, day, night, and test. The day position places all components associated with the holdup alarms or shoplifting devices into operation while turning off the sensors on doors. Obviously, the same position can be used to operate specific zones (such as an alarm zone for an unmanned storeroom) and not only holdup sensors. The control unit should provide visible displays such as lights or meters that clearly indicate the operating status of the intrusion alarm system.

For obvious reasons, the control unit within your premises should be in a location that is accessible only to you and your authorized employees.

In addition to the master control unit, used to set the intrusion alarm system to its desired operating mode, you may wish to use a remote off-on switch. This is normally installed on the exterior of the building near the door you routinely enter and leave when the building is unattended. It enables you to turn the system

off when you enter in the morning, and to activate it from the outside at night.

Alarm systems connected to central stations do not normally use a remote control switch. Rather, the system is turned on and off by the central station; the individual operating the system notifies the central station when he leaves, and any alarm is disregarded. In the morning, a signal is transmitted to the central station when the alarm is switched to the day position, and the central station knows that the entry was by an authorized person, even though the system sent out an alarm when the door was unlocked and opened.

Some alarm systems incorporate a feature referred to as an exit delay. With this feature, the alarm system does not enter the secure mode (armed and ready to respond) for a period of time such as 15, 30, or 45 seconds after it has been activated. This allows the operator sufficient time to leave the premises without causing an alarm to sound when he opens the door to leave. Such systems may also incorporate an entrance delay, which will permit the alarm to be shut off before a signal is transmitted when entering the premises.

Correct opening and closing procedures are essential when a remote alarm system is connected to either a police department or a central station.

Tamper Protection

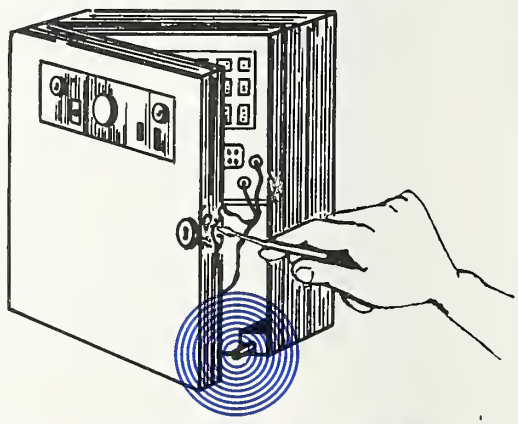
A sophisticated intruder often has a working knowledge of alarm systems and components. Such an intruder is capable of disabling an alarm system if he has access to circuitry or adjustment controls. For example, a switch sensor that is used in a normally closed circuit, the most popular method of wiring, can be defeated by simply connecting a jumper wire across the contact terminals.

Tamper protection is a desirable feature for intrusion alarm systems used in commercial applications. The simplest method of providing some degree of protection is by the use of tamper switches. The tamper switch is usually a mechanically actuated switch that is mounted within the equipment enclosure or cabinet. The switch signals an alarm if the cover is opened. In addition to their use on cabinets, tamper switches are also used in sensor enclosures and in control units.

Exposed wiring between components is also vulnerable to tampering, and for that reason many alarm systems incorporate line supervision, particularly between the control unit and the central station or police department receiving equipment. This is accomplished by means of a separate alarm circuit that monitors the impedance of the lines. An end-of-line resistor is often used for this purpose and is wired in parallel across the terminal at the point where the wire is connected to the control unit, or to a component. This resistor provides a fixed reference impedance that will change if the wires are cut, or if jumper wires are connected to the lines. An alarm will be transmitted if the impedance changes by more than a specified amount.

Line supervision also makes it possible to detect problems, such as a line that has been damaged by a severe rainstorm, by means of the transmission lines themselves.

Other types of line supervision are also used and include the transmission of coded signals between components for very high security systems. This type of supervision enables one to check the status of the various components and locate line problems, or to detect attempts to introduce external signals into the transmission line in an effort to defeat the system.



A tamper protection device sets off an alarm when an intruder tries to defeat a protected component of the alarm system—in this case, the control unit.

INSTALLATION AND OPERATIONAL CONSIDERATIONS

The proper installation and operation of an intrusion alarm system are the keys to its effectiveness. Even good components, appropriate for the application but improperly installed and operated, will perform poorly. The result of improper installation can be a system that quickly becomes an annoyance by constantly generating false alarms or one that provides little protection. As with any electromechanical system, proper maintenance is required on a routine basis.

Environmental Factors

Building vibrations induced by wind, vehicles moving outside the building, or heavy machinery are troublesome to most sensors. In fact, excessive vibration will cause a motion detector to signal a false alarm. In most sensors there can be a gradual loosening of adjustment or alignment screws that will impair the operation of the unit. Vibration of a photoelectric unit could change the aim of the beam and result in less than optimum operation. As previously mentioned, there are several sensors that are designed to signal an alarm in response to vibration and the effect of extraneous vibration upon such devices is obvious.

Temperature and humidity must also be taken into account. Sensors installed in an uncontrolled temperature area (such as a garage, a warehouse, or a barn) may be subjected to extreme temperatures that are not within their operating range. It is difficult to predict the effect that temperature or humidity will have upon a particular sensor. One unit may cease to function, while another may decrease in detection sensitivity so that the unit is no longer reliable and yet a third could increase in sensitivity so that an alarm would sound constantly. Excessively high or low humidity can alter the detection characteristics of ultrasonic motion detectors and capacitance sensors. If you intend to install alarm system components in areas with extreme temperature and humidity variations, the equipment specifications should be carefully examined. If the manufacturer cannot assure you that the equipment will operate satisfactorily in your environment, look for another supplier.

Electromagnetic interference is another problem that is common to all equipment. Radiated interference can be due to transmission sources such as patrol car radios, or it can come from natural disturbances such as electrical storms. With few exceptions, the equipment that has been tested by the Law Enforcement Standards Laboratory was susceptible to electrical fields of the type produced by police radios, other emergency communication equipment, taxicab communications, and radio or television stations. The problem is minimized when the equipment is mounted in a building that provides electrical shielding because of metal construction or reinforcing steel. If your business is located near a TV station, you should be aware of the potential problem and discuss it in detail with the installer. You should also keep this problem in mind if you employ internal guards who use portable transceivers. Perhaps you will find it necessary to identify specific areas within your premises where transmission is prohibited.

The second type of electromagnetic interference is conducted, or power line, interference. When a compressor motor starts, or other equipment is turned off and on, it can induce a voltage surge in the power lines within your building and cause the system to generate an alarm. Fortunately, most alarm components are not overly susceptible to this type of interference. However, it is a good idea to connect alarm components to a separate electrical circuit. There is a simple test that you can make if you suspect that an alarm component is susceptible to conducted interference. Plug a normal desk top fluorescent reading lamp (one with a separate ballast unit) into the same line as the component and turn the light on and off rapidly. If the component enters the alarm state, the chances are that it is not very resistant to power line interference as a source of false alarms.

A momentary drop or increase in the line voltage is also a potential problem for an alarm system. Most of the equipment tested by the Law Enforcement Standards Laboratory operated satisfactorily over a range in line voltage from 85 to 110 percent of the rated voltage. If you anticipate a wider range of voltage, it is suggested that you check with the supplier before you purchase the equipment.

Sensor Installation Factors

Selecting components that are suitable for the intended use, compatible with the operating environment, and installing them in accordance with the manufacturer's instructions will afford you an intrusion alarm system that will provide trouble-free, effective protection.

Before you install any sensor in an area that you believe to represent a marginal application for the device, try to use a test unit at the location on a temporary basis. Let it operate for a few days and see if it performs the way it should before you install one as a permanent part of your system.

Perimeter or Linear Protection. The most popular switch sensor is the magnetic switch. When considering a magnetic switch for use on a steel door and frame, make certain that it is designed for such use. In some cases, it might be necessary to mount the switch on special spacer blocks that place the switch and magnet a sufficient distance from the steel surface to allow proper operation. After a balanced magnetic switch has been mounted in its permanent location, it will be necessary to adjust the balancing magnet. In some instances you might wish to have versatility, so that a window can be partially open for ventilation and yet be protected by the switch sensor. This can be accomplished by mounting a magnetic switch in a suitable location with the window open and a magnet positioned directly opposite the switch. A second magnet is then mounted so that it operates the switch with the window closed.

The movement or displacement required to actuate a magnetic switch is important. If the switch is actuated by a very small displacement, it may cause false alarms when the wind or normal building vibration causes loosely fitting doors or windows to rattle. This is also a common problem with mechanical switches. Obviously, the switch should sound an alarm before the displacement is so great that one can enter or reach in and tamper with the switch.

Normally, mercury switches are used only for a window or trap door, such as a transom, that opens by pivoting around a horizontal axis. It will be necessary to adjust the switch after mounting so that it actuates when the door or window has been tilted to the maximum permissible position. Since a mercury switch is mounted on the moving member, rather than the window frame or door jamb, the connecting wire is subjected to the stress of bending each time the window or door is opened or closed. In such instances, the installer will normally use a door cord, which is a special wire designed to withstand repeated bending. Door cords are also used to make connections to metallic foil on swinging glass doors.

Photoelectric sensors require careful alignment of the optical system, particularly if the system uses mirrors to route the beam. The transmitting and receiving units as well as the mirrors must be rigidly mounted and the adjustment should incorporate a clamping mechanism to retain alignment once the system has been set up. While some of these units are contained in housings that are mounted flush with the surface of the wall, others are mounted on the surface of the wall. Such units are subject to unintentional shocks, as from cleaning personnel using brooms, etc., that could disturb their alignment. Most of the tested photoelectric units have performed well; however, proper alignment was difficult to achieve with some of the units.

Point, Spot, or Object Protection. Sound sensors and microphone vibration sensors designed to respond to attempts to penetrate or break through walls are most often used to protect vaults and similar massive structures. These devices have been found to perform reasonably well when installed and operated in accordance with the manufacturer's instructions. The use of these devices in other applications should be carefully considered, because normal structural vibrations and noise

from aircraft, trains, trucks, etc. may induce sound levels and vibrations of sufficient intensity to cause false alarms.

Contact vibration sensors are used primarily for vault protection. These devices aré inexpensive and can be quite useful; however, care must be exercised when installing them. Some manufacturers recommend installation with pressure sensitive tape, which can change the vibration response characteristics of the device; the overall response might also change as the tape ages. It is better to use several of these devices to protect a length of wall than to use a single unit set to a very high sensitivity. Their placement with respect to structural members as well as the construction of the wall are important. These devices are not precision devices and rely upon spring tension for the adjustment of vibration sensitivity. Tests have proven that contact vibration sensors are quite difficult to adjust for proper operating sensitivity.

Capacitance sensors use the metal object being protected as one plate of a capacitor. These objects, such as filing cabinets or safes, must be electrically insulated from earth ground or the ground of the building. Units are available with both fixed and variable capacity and in a range of sensitivities that will allow as many as a dozen file cabinets to be protected by a single unit. It is important to make good electrical contact with the item that is to be protected. Many of these units incorporate an automatic compensation circuit to accommodate changes in the room environment, such as temperature and humidity, which can affect the sensitivity of the detector. Be sure to obtain this feature if the equipment is to be used in a room that is not temperature controlled. The majority of the capacitance sensing equipment that was tested performed well in all respects.

Area, Space, or Volume Protection. Microwave motion detectors transmit energy that will penetrate many materials. To avoid false alarms, you will want to contain the detection field within a single room or area. Thus, if the building has large display windows, or drywall partitions, you must select the antenna pattern carefully. Metal surfaces or objects will reflect the energy, causing large distortions of the normal pattern, and it is not uncommon to find that motion is detected in areas that are not expected to be included in the antenna pattern. If the energy escapes to the exterior of the building, pedestrians, moving vehicles, and swinging signs can all become sources of false alarms.

Because it is possible to use an antenna capable of producing a narrow beam that extends more than a hundred meters (several hundred feet), the microwave detector can be used to detect motion anywhere within a long corridor in a building. Similarly, some installations have taken advantage of the fact that the energy will penetrate building partitions and so have used a single detector to protect two or more rooms. A satisfactory installation of this type can be difficult to accomplish, particularly if the rooms have metal desks or furniture, or other potential reflection surfaces.

Tests of microwave motion detectors have shown that some are quite sensitive to vibration, and many will generate false alarms in response to a flickering fluorescent light. Draperies that are set into motion by heating or air conditioning air currents are also a source of false alarms.

Ultrasonic motion detectors are more frequently used than microwave motion detectors. Since ultrasonic energy is transmitted directly by the air within a room, air currents themselves can be a source of false alarms and a unit should not be installed close to a ventilation duct. Moving draperies can also cause false alarms and some units operate on a frequency that is present in the ring of a telephone bell, another source of false alarms. Similarly, a false alarm can be caused by a squeaky hinge, by air being sucked beneath a closed door by a vacuum cleaner, or by escaping steam. While ultrasonic energy is generally well contained within a room, it is possible that small amounts of the transmitted signal can pass through cracks, under doors, etc. If separate ultrasonic motion detectors are used in adjoining rooms, make sure that both units operate on the same frequency, and synchronize the transmission of the two signals.

Infrared motion detectors must also be mounted on surfaces that are not subject to building vibration. Tested units have performed well,

although alignment was sometimes difficult. Most of these detectors are not sensitive to sunlight passing through window glass; however, some will respond to small beams of direct sunlight reflected from moving venetian blinds or from the floor. Try to locate such detectors so that they are not exposed to reflected energy sources.

After the Installation

Once the individual sensors have been installed and connected to the control unit, it will be necessary to adjust them for proper operation and then test each sensor to be sure that it is working as intended. Your control unit should have a test position that will allow each component to be tested without sounding the alarm.

Pay particular attention to the motion detectors and their adjustment. Any electronic device will demonstrate less than best performance if it is pushed to its electronic and sensitivity limits. Some installers have made the mistake of attempting to use a single ultrasonic sensor to provide protection for an area that is slightly larger than it was designed for. This can be done by adjusting the sensitivity to its maximum setting, but will result in a system that false-alarms routinely. The only solution is to reduce the sensitivity, which means that portions of the room will no longer be protected. Similarly, if an ultrasonic or microwave motion detector is installed in an environment that contains false alarm stimuli, often the first action taken is to reduce the sensitivity in hopes of eliminating the problem. It is not uncommon to find that the sensitivity has been reduced more than once, and the unit is finally set at a sensitivity so low that the detector will not sense the presence of an intruder.

When you use motion detectors, it is desirable to use those that incorporate a visible walk-test indicator. This can be a light which, when the unit is switched to the test mode, comes on whenever the detector enters the alarm state. A meter can be used instead of a light. You can then walk throughout the room and observe whether your motion has been detected. When you perform this test, walk only two or three steps and stop. Once the detector has alarmed, you will have to wait a few seconds until it resets and the indicator goes off before you try another test.

ONCE INSTALLED
√ ADJUST
√ TEST (on normal & standby power)
√ INSPECT
√ MAINTAIN
ALL PARTS OF SYSTEM

If any of the components of your alarm system include tamper protection circuits, be sure that the installer demonstrates that these circuits are operational. While not a common occurrence, there have been occasions when installers have neglected to connect the tamper protection circuits of alarm systems and it was not discovered until the systems had been compromised by an intruder. Similarly, make sure that the system operates properly on standby power, if this capability is provided.

When the installation has been completed to your satisfaction and you assume the responsibility for its daily use, be sure you establish and follow a routine maintenance schedule in accordance with the manufacturer's recommendations. The batteries of wireless systems will have to be checked periodically and replaced on a fixed schedule, usually about once a year. Similarly, standby power supplies must be checked and nonrechargeable batteries replaced on a fixed schedule. Rechargeable batteries normally have a life-time of many years.

Some components may require periodic cleaning to remove dust or other accumulated foreign matter, and many will require minor electronic adjustment from time to time.

All of the sensors should be tested on a routine basis to be sure that they remain operating, for equipment failure is always a possibility. For example, laboratory tests have established that it is not uncommon for mechanical switches, and to a lesser extent magnetic switches, to fail

after a limited number of opening and closing cycles. While a minimum of 100,000 cycles of operation without failure is considered to be mandatory for alarm system use, a switch can fail after as few as fifty cycles of operation.

The other system components should also be checked periodically. Examine door cords to be sure that the terminal block connections are still tight, and that the cords are not showing signs of wear. If you use window foil, be sure that normal cleaning operations have not damaged the protective coatings or the adhesive that bonds it to the glass. Be sure to check sensors mounted on brackets or otherwise attached to the building to see if bolts or screws need to be tightened. If you use money clips in cash drawers, carefully examine the lead wire for evidence of wear. This wire is subject to constant stress as the drawer is opened and closed, and it is not uncommon for the wire to break from fatigue.

The periodic inspection of the entire system will also ensure detection of any evidence of attempts to tamper with it, alerting you to the fact that someone may be planning to break into your facility.

Unless you have a large and complex intrusion alarm system, routine maintenance and inspection is neither difficult nor time consuming. Frequently, the maintenance and inspection of the intrusion alarm system will be a part of an overall service contract, relieving you from this responsibility.

SOUNDING THE ALARM

The type of alarm signaling/transmission system you should use in your particular application depends upon the location of your place of business, the frequency of police patrols, and your ability to afford the cost. Remember that, after deterrence, the purpose of an alarm is to summon the proper authorities to stop a crime during the act of commission or lead to the apprehension of the intruder. To this end, it is important that the response to the alarm comes in the shortest possible time.

Four types of alarm signaling systems are in general use: the local alarm, the central station system, the automatic telephone dialer system, and the direct connect system. It is advisable for you to check the local ordinances and codes concerning electronic intrusion alarm systems. There may be regulations governing the types of alarm systems that you can install, to whom the alarm may be transmitted, or the length of time a local alarm can be sounded.

Local Alarm System

Local alarm systems provide on-the-premises indications, usually by means of bells or lights, that an attempted or successful intrusion has taken place. You are, therefore, relying on someone hearing or seeing this signal and calling the responsible authorities. In today's densely populated urban regions the local alarm may often go unnoticed or fail to elicit any responsible reaction. In less populated areas, there may be fewer chances that someone in your neighborhood will be present to hear the alarm; therefore, the appropriateness of a local alarm is sometimes questionable.

The local alarm also serves to notify the burglar that he has been detected. This may be advantageous in frightening off the less experienced intruder before he can finish his intended act. On the other hand, during a holdup for example, a local alarm indication may provoke the robber and cause him to harm people in the area.

A local alarm system is less expensive than other types. It does not require the leasing of telephone lines for the transmission of signals; the equipment itself is often relatively simple, unsophisticated, and less expensive to install and maintain. Because of their simplicity, however, local alarm systems can be defeated by a burglar with relatively little trouble. Law enforcement officials generally prefer one of the silent forms of alarm transmission. In some areas, so remotely located that neither police nor private security agencies could reach the scene in time to apprehend an intruder, the local alarm is probably the only practical type of alarm to use, in hopes of frightening the intruder away or alerting a chance passerby.

Some intrusion alarm systems use a local alarm in combination with a remote (silent) alarm. In these installations, the silent alarm is transmitted immediately when a sensor is actuated. The local alarm is generally sounded on a delayed basis, usually several minutes after the silent alarm has been transmitted. This alarm sequence is intended to give the police time to respond to the alarm, while minimizing the time that the intruder has to perform his criminal act. There are also intrusion alarm systems that sound a local alarm simultaneously with the transmission of a silent alarm.

Central Station System

If you choose a commercial central station system to supply your intrusion alarm needs, a signal indicating an attempted intrusion on your premises will be sent directly to a remote, continuously staffed supervisory station, usually by way of a leased telephone line. The demand for leased, or dedicated, telephone lines is so high in many localities that alarm companies have a difficult time obtaining them. As a result, some central station systems will use a "McCulloch loop" for transmission. This equipment allows 12 or more alarm subscribers to share a single leased line. Such systems are only slightly less secure than a direct wire connection, and may result in a decrease in the monthly leasing costs. Since leased wires are expected to become increasingly difficult to obtain, future installations will be forced to make increasing use of shared lines, and the alarm companies may also find it necessary to use radio transmission of the alarm signals.

Since a central station alarm system is a commercial service, the degree of protection you use will determine the price you pay. The types of services offered range from the monitoring of alarm signals and notification of the law enforcement authorities to dispatching private guards to your premises when an alarm has been transmitted. Central station systems usually maintain and repair the equipment they provide. Commercial services of this type usually employ well-trained personnel. Typically, however, you have less authority over the operation of the system and may not know the system is in need of repair. Similiarly, unless the central station informs you, you may not be aware that there has been a telephone line failure during a certain period of time. Often central station personnel are given keys to the protected premises so that they may enter in case of an alarm. While central station services are probably the most highly supervised, you will find that they are also the most expensive.

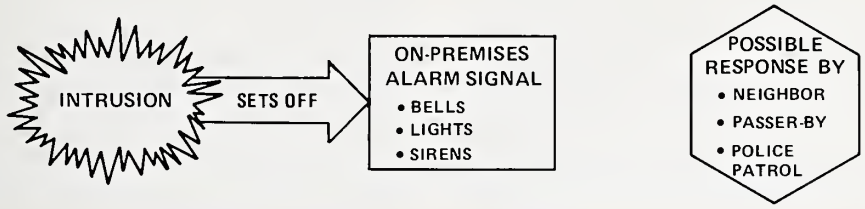
Automatic Telephone Dialer

Two types of automatic telephone dialers are available, the tape dialer and the digital dialer. Dialers offer the advantage of using less costly public telephone lines instead of leased lines and may be adequate for low security applications. A tape dialer can deliver a prerecorded or coded message to a central station office, to a private answering service, to a neighbor, to yourself, or (if local ordinances permit) directly to the police. Many of the earlier tape dialers were a source of constant problems to police departments. Since these devices were quite unsophisticated, they would dial the number of the police department and automatically start to play the prerecorded message after a specific time delay, generally a period of time equal to the time required for the telephone to ring three or four times. It was not uncommon for the dialer to play most of the message before the police were able to answer the phone. As a result, the police knew that an alarm had been sent, but did not know its location. In addition, these systems often seized the police telephone line, and would keep the line open until physically shut off at the dialer unit itself. Thus, the police department telephone lines were tied up for extended periods. In addition, it was common for the tape transport mechanism to malfunction and deliver no message at all.

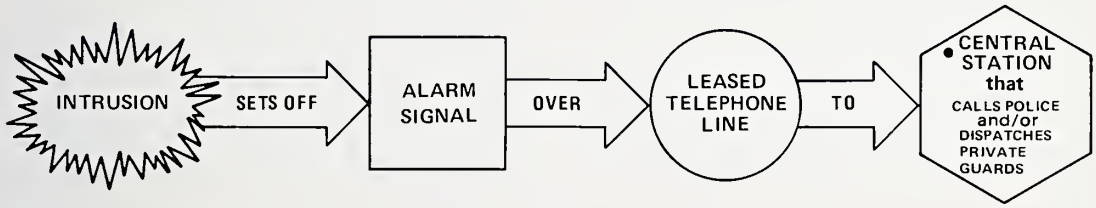
Most modern tape dialers have solved the problems of the earlier units, and are reasonably reliable. Many include circuits that delay the message transmission until the telephone being called is actually answered. In fact, most dialers are capable of dialing two or more numbers in the event that the first one dialed is busy or does not answer. Many of the dialers also permit the transmission of fire alarm messages through a separate channel. Some

ALARM SIGNALING/TRANSMISSION SYSTEMS

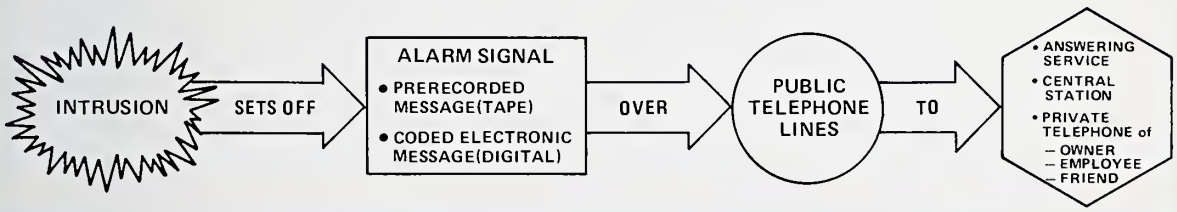
LOCAL ALARM SYSTEM



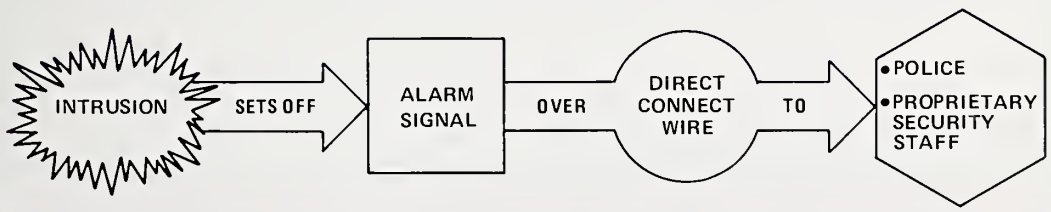
CENTRAL STATION SYSTEM



AUTOMATIC TELEPHONE DIALER SYSTEM



DIRECT CONNECT SYSTEM



tape dialers also include circuitry that prevents the dialer from being defeated by incoming calls on the dialer's line.

The digital dialer does not use a recorded tape message. It is a solid state, electronic device that transmits the alarm message as a series of coded electronic pulses. This alarm signal can only be received by an electronic terminal that can process and decode the message, translating it into a form that can be interpreted by the individual monitoring the receiving equipment. In some instances the alarm is typed out by Teletype equipment, while in others it is directed to a conventional alarm display. The digital dialer equipment offers distinct advantages, for it is possible to include circuitry that allows the receiving station to provide line supervision, and to check the status of the dialer on a routine basis.

In some cases, the receiving terminals for digital dialers are connected to small computers that provide additional data such as the type of establishment, location of alarm sensors, etc., to be displayed for the operator.

Because a special receiving terminal is required, digital dialers are used almost exclusively in central station alarm systems. A few police departments, however, have installed receiving terminals that will accept alarms from digital dialers.

Since both tape and digital dialers use normal telephone transmission lines, their use is subject to approval by the telephone company. In some cases, the telephone company may require that a coupling circuit be leased directly from them, while in others, it may be acceptable to install a coupling circuit (modem) that meets with the telephone company's approval, but is not purchased or leased directly from them.

Direct Connect System

In a direct connect system, your intrusion alarm system is directly connected by wire to a remote alarm receiver located either at police headquarters or at some other location. Unless your establishment is a financial institution, local ordinances may not permit direct reporting to police stations. A variation of this concept is the

TABLE 3. THE RELATIVE EFFECTIVENESS OF PROTECTION SYSTEMS

	ROBBERY	BURGLARY	THEFT
PHYSICAL PROTECTION* (NO ALARM SYSTEM)	○	○	○
COOPERATIVE SYSTEM	⊗†	●	●
LOCAL ALARM	○†	⊗	⊗
AUTOMATIC DIALER	⊗†	⊗	⊗
DIRECT CONNECTION TO POLICE	●†	●	●
CENTRAL STATION	⊗†	●	●
PROPRIETARY SYSTEM W/ IN-HOUSE SECURITY FORCE	●†	●	●

● EXCELLENT

⊗ GOOD

○ FAIR

*The effectiveness ratings assume that the protected premises have adequate physical security. If not, each rating should be reduced one level, e.g., from excellent to good.

†Assumes that someone other than the victim can actuate the alarm.

cooperative or "buddy" alarm system. In this system the alarm signal, either by direct wire or through the use of an automatic telephone dialer over the normal telephone lines, goes to a nearby business establishment or residence where a designated individual receives the signal and phones the appropriate law enforcement agency. In this case you should be certain that the one who receives the alarm signal knows the proper procedures for notifying the police.

The charges for leasing telephone lines for alarm system applications, which are usually regulated by public service or utility commissions, involve a small fraction of the total cost of your system; in many localities there are several grades of lines available, at varying costs. The cheapest alarm lines are not as good as the voice grade lines. While the actual charge for leasing a telephone line varies from area to area, there is usually a nonrecurring installation charge and a monthly service charge. If you decide to use a central system service, the telephone line charges are billed to the central station and added to your contract.

GETTING YOUR MONEY'S WORTH

As discussed earlier, the economics of installing an intrusion alarm system involves a business decision that only you can make. The factors that enter into this decision are numerous, and the bottom line of the analysis is the cost to install and operate the system that meets your needs. It goes without saying that, as a businessman, you want to get your money's worth.

The first step in achieving this goal is to be certain that you have properly evaluated your security needs. The flow chart on page 36 serves to outline the steps that enter into the selection of an optimum intrusion alarm system. Use this chart as a means of insuring that you have not overlooked any factors that should be considered. *Table 3,* the comparison of the relative effectiveness of the various types of protection, and *Table 2,* the brief summary of the advantages and disadvantages of the various sensors with respect to their use in different applications, will also be convenient references.

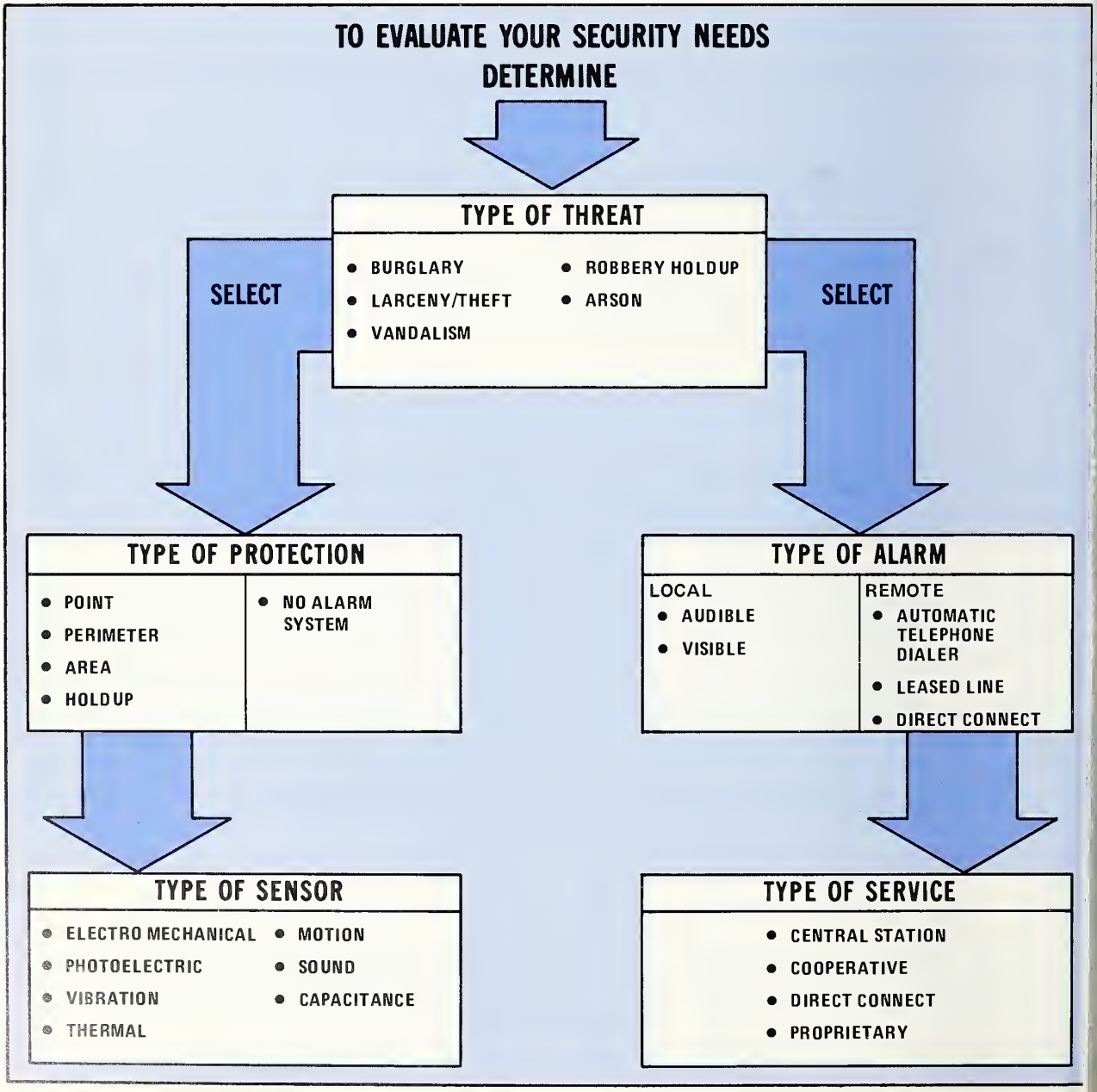
The cost of installing and operating an alarm system will vary significantly depending upon the type of system and the community in which your business is located. As a rule of thumb, you can expect that the cost of installation will be approximately equal to the cost of the components that make up your system. Each alarm installer will have his own method of estimating the price of the system. However, whether or not each item is separately costed, the bid should clearly identify the components that will be used and where they will be located on the premises. Thus, regardless of the bid method, you will be able to compare the systems that are proposed. Obtain quotations from several alarm installers, and get all quotations in writing.

Investigate the firms that you ask to provide quotations. In addition to checking with the Better Business Bureau, ask for references, and ask your local police if they have had particularly good or bad experiences with any firm that you consider hiring to provide your system. Make certain that the firm has the proper license if your community requires one. In addition, check to determine whether the local installers are members of trade associations. There are several national and regional societies or associations open for membership to alarm companies and installers. These associations attempt to keep their members current with alarm system technology, and within limits (as with any voluntary membership organization) they attempt to insure that their members uphold high standards of business practice.

There are two methods for procuring an alarm system: buying and leasing. There are responsibilities as well as advantages in direct ownership of the equipment. For example, although you make a larger initial cash investment in purchasing the system, you will be

able to depreciate the cost of the hardware. You must also realize that the sophisticated electronics involved in many systems will require periodic maintenance (this is applicable whether the system is purchased or leased). In leasing a system, maintenance is usually provided as needed and periodic inspections are made. Therefore, you should consider all the costs (that is, purchase price versus initial leasing costs, service contract costs versus periodic maintenance, etc.) over the number of years you feel the system will be in operation.

You are considering the use of an electronic intrusion alarm system because of the value of your property and merchandise as well as the value of human life that may be involved should a robbery take place on your premises. Thus, beware of "bargain" systems. Such systems may prove unworkable or easily defeated by an intruder. Prior to signing a contract for any service you should also make certain that the alarm system company with whom you are dealing will provide maintenance or service on a continuing basis.



☆ U.S. GOVERNMENT PRINTING OFFICE : 1979—O-297-567

ANNOUNCEMENT OF NEW PUBLICATIONS ON NATIONAL CRIME AND RELATED SUBJECTS

Superintendent of Documents,
Government Printing Office,
Washington, D.C. 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued on the above subjects (including this NBS series):

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification Key N-538)

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

SPECIAL FOURTH-CLASS RATE
BOOK