A STUDY OF THE USE OF CLOSED CIRCUIT TELEVISION AND INTRUSION DETECTION EQUIPMENT IN INDUSTRIAL PLANT SECURITY

Thesis for the Degree of M. S.
MICHIGAN STATE UNIVERSITY

Thomas Gerald Nicholson

1963

A STUDY OF THE USE OF CLOSED CIRCUIT TELEVISION AND INTRUSION DETECTION EQUIPMENT IN INDUSTRIAL PLANT SECURITY

By

Thomas Gerald Nicholson

AN ABSTRACT

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

School of Police Administration and Public Safety

1963

Approved:

Dr. Leon H. Weaver, Chairman

Mr. Raymond T. Galvin, Member

Mr. Roy L. Holladay, Member

ABSTRACT

A STUDY OF THE USE OF CLOSED CIRCUIT TELEVISION AND INTRUSION DETECTION EQUIPMENT IN INDUSTRIAL PLANT SECURITY

by Thomas Gerald Nicholson

Closed circuit television and intrusion detection equipment have been used in industrial plant security for several years. In spite of this fact, there is limited objective information available which can be used by security directors in making decisions on use of such equipment. The bulk of the available literature consists of government publications, sales brochures, and short articles in a variety of periodicals.

Contrary to popular belief, electric intrusion detection equipment has been in use for over 100 years and new developments are being introduced each year.

All intrusion detection systems in common use today have three basic components: a sensing system, signal wires, and monitoring equipment.

The use of closed circuit television in industrial security is relatively new. It is anticipated that as reliability of the equipment improves and costs are reduced its use will increase significantly.

Closed circuit television systems consist of three basic parts: the camera or "eye" of the system, the

interconnection system, and the monitor. A basic understanding of each part is necessary in order to employ the equipment successfully.

Interviews were conducted with security directors of industrial facilities to determine the effect of use of such equipment on security guard effectiveness; guard personnel requirements; level of security provided; and security costs.

As a result of these interviews it was found that, in the opinion of the directors interviewed, use of the equipment can: (1) Increase the effectiveness of a guard force. (2) Permit reduction of the total strength of the guard force without reducing the protection provided. (3) Result in monetary savings after considering the total cost resulting from use of the equipment. Use of the equipment will not inevitably produce these results but, with proper planning, selection of equipment, and employment, these results can be achieved.

A STUDY OF THE USE OF CLOSED CIRCUIT TELEVISION AND INTRUSION DETECTION EQUIPMENT IN INDUSTRIAL PLANT SECURITY

By

Thomas Gerald Nicholson

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

School of Police Administration and Public Safety

1963

TABLE OF CONTENTS

CHAPTER PAGE

I. THE PROBLEM AND DEFINITIONS OF TERMS USED . . . 1

The Problem 1

Statement of the Problem. 1

Statement of Hypotheses 1

Importance of the Study 2

Methodology 5

Definitions of Terms Used 8

II. REVIEW OF THE LITERATURE. 9

Literature on Closed Circuit Television . . . 9

Literature on Intrusion Detection Equipment . 10

III. INTRUSION DETECTION SYSTEMS 13

History and Development of the Intrusion Alarm Industry 13

Alarm System Components 21

Sensing System. 22

Electromechanical Detectors 23

Audio Detectors 28

Photoelectric Detectors 32

Capacitance Detectors 38

Sound Wave Detectors. 44

Signal Wires. 51

Monitoring Equipment. 54

Receiving Alarms. 54

Line Supervision. 55

CHAPTER PAGE

Current Supply. 57

Location and General Types. 57

Recent Intrusion Alarm Developments 59

Detection Devices 60

Alarm Transmission Equipment. 63

The Role of Underwriters' Laboratories. . . . 64

IV. CLOSED CIRCUIT TELEVISION 69

Development of Closed Circuit Television. . . 70

Components of a Closed Circuit System 73

Camera. 74

Interconnection System. 78

Monitor 79

Security Applications 81

Identification. 82

Vehicular Control 85

Area Surveillance 86

Discussion. 89

V. LIMITATIONS OF THE STUDY. 91

VI. ANALYSIS. 95

VII. CONCLUSIONS AND PROBLEM AREAS WHICH NEED ADDITIONAL STUDY 101

Conclusions 101

Problem Areas Which Need Additional Study . 104

BIBLIOGRAPHY. 107

APPENDIX A. Sample Interview Schedule. 116

APPENDIX B. Recapitulation of Responses to Interview Questions 119

CHAPTER I

THE PROBLEM AND DEFINITIONS OF TERMS USED

Closed circuit television and intrusion detection equipment have been used in industrial plant security for several years. There is limited objective information available which can be used in making decisions on the use of such equipment. It has been claimed that security costs can be reduced through its use but this claim has not been subjected to critical analysis and evaluation.[1] One of the purposes of this study is to provide such an analysis and evaluation.

I. THE PROBLEM

Statement of the Problem. In this study descriptive information on closed circuit television and intrusion detection equipment and their applications in industrial security will be presented. In addition, an attempt will be made to determine if the use of such equipment can increase the effectiveness of a guard force and permit reduction of this force, thus reducing security costs without reducing the level of security provided.

Statement of Hypotheses. In order to determine

---

[1] "Saving Big with Robot Guards," Factory, CXV (May, 1957), 74.

the effect of use of the equipment on security guard personnel requirements and resultant monetary savings, the following hypotheses are established and will be tested in the study: (1) Closed circuit television and intrusion detection equipment can be used to increase the effectiveness of a security guard force. (2) This increased effectiveness will enable management to reduce the total strength of the security guard force without reducing the protection provided; or redistribute guard force manpower to provide additional security or services. (3) If the firm elects to reduce the total strength of the guard force, it can result in monetary savings after considering all costs involved in using the equipment.

Importance of the Study. Industrial plant security has become a big business in this country. It has been estimated that management spends $250,000,000 each year to reduce losses but industrial thefts still exceed four billion dollars per year.[2]

In addition, the international situation is such that classified national defense information and material in the hands of private industry must be protected from sabotage, espionage, and other subversive activities.

Firms with a defense mobilization potential should also establish some security measures to preclude an abrupt

---

[2]"Automate Plant Protection," Factory, CXIX (December, 1961), 60.

transition from peace to wartime security measures. Such measures will also serve to prevent larceny and deter foreign agents in their attempts to gather information on national preparedness.

American industry is highly competitive, not only with other American firms, but with firms of other countries. Large fiscal outlays are made each year for research and development designed to keep firms in a competitive position in national and international markets. In many cases this research produces knowledge which cannot be patented because it is in the form of "trade secrets" or "industrial know-how." In other cases the fruits of research are patentable but could be used by firms in other countries which do not protect American patent rights. It is thus necessary for such firms to establish security measures to protect these assets gained through a costly research investment.

After determining that security measures are necessary to comply with government regulations or as a means of corporate "self-preservation" the next question is: How can this be done most effectively at minimum cost? One possible answer might be through use of closed circuit television and intrusion detection equipment in combination with other security measures.

Before a decision is made to determine if the equipment will be used management must determine if it is feasible for use in their specific facility. In order to do

this management must know something of the types of equipment available, and their principle of operation, capabilities, and limitations. If it is determined that the equipment will provide the necessary protection, then it is necessary to compare relative costs of the equipment with other security measures.

Since it has been estimated that one 24 hour guard post costs $25,000 to $30,000 annually, the effect of the use of such equipment on guard personnel requirements is an important consideration in comparing costs.[3]

Now that the basic information requirements have been established, the next step is to find a source which will provide reliable information which can be used in making a decision. At this point the real problem begins. Manufacturers of closed circuit television and intrusion detection equipment will furnish sales brochures, descriptive material, and advice on use of their equipment. They may also provide "proof" of savings through use of the equipment. Since this is designed to induce sales, the objectivity of the information is questionable.

Firms which have access to classified defense information can secure advice from their respective cognizant security officers who have access to government publications.

If the firm has a defense mobilization potential,

---

[3] Ibid.

it may be listed on the Key Facilities List and may secure the advice of a Department of Defense representative who also has access to government publications.

In the event the firm does not fall into one of these categories, a limited number of government publications are available which can be purchased directly from the Government Printing Office. In addition, the firm can obtain literature from Underwriters' Laboratories, a non-profit testing organization.

There is even less information available on security applications of closed circuit television. Manufacturers of television equipment will provide some information but this is usually related to general, rather than security, applications.

It should be noted that objective information which can be used in making a decision on the use of closed circuit television and intrusion detection equipment in security systems is very limited. The purpose of this study is to provide additional information upon which to base such a decision. The study will include information on types of equipment available, their principle of operation, and capabilities and limitations. Information concerning the increased effectiveness of the guard force, personnel requirements, and relative costs will also be presented.

Methodology. In order to gain information for the descriptive portion of the study, manufacturers of intrusion detection and closed circuit television equipment were

solicited by mail and information on their equipment was studied. Periodical indexes were screened and all references to burglar alarms, intrusion detection equipment, and security applications of closed circuit television were screened and evaluated.

To test the hypotheses, interviews were requested at all known industrial facilities in Wayne County, Michigan, which use closed circuit television and/or intrusion detection equipment in their security systems. This area was selected because it contains the city of Detroit, which is highly industrialized, and thus kept travel and expenses at a minimum. The list was compiled by contacting members of the American Society for Industrial Security and other persons in the Wayne County area that are interested in industrial security. A total of 10 such facilities were identified and of this group 7 agreed to permit interviews.

At each facility the security director or his representative was interviewed through use of an interview schedule (appendix A) to answer questions concerning increased effectiveness of the guard force, effect on personnel requirements, and relative costs. In addition, general information on field applications of the equipment was obtained through open-end interview and personal observation.

In order to prevent use of actual names of firms visited, a code letter was assigned to each and is used for identification in the study.

It was realized at the outset that persons interviewed

could be biased in their view toward use of the equipment. In some cases the person interviewed was responsible for purchase and installation of the equipment and would thus be reluctant to admit its shortcomings. In addition, some security directors feel that their status in the company is closely related to the number of men under their supervision. This would cause them to be hesitant in admitting that the equipment could make possible a reduction of guard force personnel. These conditions were overcome to some extent by assuring the person interviewed that disclosures were in confidence and the names of persons and firms would not appear in the study.

In the case of firms which were inspected by a federal government representative an outside opinion on the relative level of security provided by the equipment was secured. In the case of firms which were not under some type of security supervision by an agency of the Federal Government an attempt was made by the investigator to make this evaluation using the same criteria utilized by such inspectors in conducting security checks.[4]

In interviews with Army, Navy, and Air Force security inspectors it was found that these determinations are made on a "common sense" basis and application of general guidance provided in the Industrial Security Manual,[5] and

---

[4]The problems encountered in attempting to do this are explained in Chapter V, Limitations of the Study.

[5]Department of Defense, Industrial Security Manual for Safeguarding Classified Information, op. cit., pp. 33-34.

another government publication listing physical security standards for industrial facilities.[6]

II. DEFINITIONS OF TERMS USED

Coaxial cable--A cable containing several wires which have a common core or axis.

Fail-safe--System designed to sound an alarm upon failure of any component of the system.

Intrusion detection equipment--Mechanical, electrical, or electronic devices which cause an alarm when entry is made into a protected area.

Lens iris--A diaphragm which mechanically limits the size of the light opening and thus has the effect of decreasing the lens diameter.

Line tolerance--The allowable fluctuation of current in an electrical system beyond which an alarm signal is activated.

Microampre--One millionth of an ampre.

Milliampre--One thousandth of an ampre.

Picture definition--The appearance of sharpness or of being in focus.

Picture stability--Continuous operation without appreciable change in the television picture.

Resolution--The ability of a television system to distinguish fine detail in the subject matter.

---

[6]Office of Defense Mobilization, Standards for Physical Security of Industrial and Governmental Facilities, op. cit., pp. 18-19.

CHAPTER II

REVIEW OF THE LITERATURE

There is little published literature available on industrial security applications of closed circuit television and intrusion detection equipment. Most of the written material is in the form of sales brochures prepared by firms that manufacture the equipment.

Literature on Closed Circuit Television. Most of the material on closed circuit television is concerned with general applications of the equipment. It is thus necessary to study these applications and devise techniques to use the equipment in a security system.

The Radio Corporation of America Service Company has prepared, under Air Force contract, a study of military applications of closed circuit television. This study includes some information on security applications.[1]

The Allen B. DuMont Laboratories has prepared an industrial television handbook which contains a good presentation explaining the basic components, principle of operation, capabilities, and limitations of industrial

---

[1]RCA Service Company, Closed Circuit Television Systems (Camden, New Jersey: RCA Service Company, 1958), pp. 183-186.

television equipment.[2]

Another book by Mayers and Chipp is also a good source of basic information on closed circuit television systems with a limited amount of information on security applications.[3]

Two articles prepared by Lee F. Malone of Burroughs Corporation give excellent descriptions of closed circuit television used to provide security in closed areas.[4,5]

Literature on Intrusion Detection Equipment. The literature in this field consists of handbooks published by government agencies, short articles in periodicals, and sales brochures prepared by firms that manufacture intrusion detection equipment.

The Army Ordnance Corps has published a technical manual designed to provide guidance for security officers at depots under the control of the Ordnance Corps. This is one of the best publications available on intrusion detection equipment. Although designed for use at military facilities, it contains valuable information which can be

---

[2]Allen B. DuMont Laboratories, Incorporated, Industrial Television Handbook (Clifton, New Jersey: George R. Epple Company, 1958).

[3]Morris A. Mayers and Rodney D. Chipp, Closed Circuit TV System Planning (New York: John F. Rider, 1957).

[4]Lee F. Malone, "Control of Closed Areas by Closed Circuit Television," Industrial Security, II (April, 1958), 8.

[5]Lee F. Malone, "Modern Electronics Assisted by Age Old Mirror," Industrial Security, VII (January, 1963), 12.

used at industrial plants.[6]

The Office of the Provost Marshal General, Department of the Army, has prepared a short technical bulletin designed to guide military police personnel in use of intrusion detection devices on military installations. This publication also contains information which can be used for industrial plant security planning.[7]

Underwriters' Laboratories publications on intrusion detection equipment include a booklet listing standards for installation, classification, and certification of intrusion detection systems.[8] This organization also publishes an equipment list of all certified equipment.[9]

The Mosler Research Products Company has prepared a booklet which contains one of the most comprehensive and objective descriptions of intrusion detection equipment that could be found. This booklet describes each type of alarm system in general use today and gives the advantages and disadvantages of each. It also contains some general

---

[6]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961).

[7]Department of Army, Intrusion Detection Devices, TB PMG 26 (Washington: Government Printing Office, 1959).

[8]Underwriters' Laboratories, Standards for Safety; Installation, Classification and Certification of Burglar Alarm Systems, U.L. 681 (Chicago: Underwriters' Laboratories, 1961).

[9]Underwriters' Laboratories, Automotive and Burglary Protection Equipment Lists (Chicago: Underwriters' Laboratories, 1962).

cost estimates for comparison purposes.[10]

Many periodical articles were found on intrusion detection equipment but they were generally repetitious and contained information on use of the equipment for burglar protection rather than use in industrial plant protection. Some of the information contained in these articles can be translated into industrial security applications but their value is limited.

Two of the Department of Defense agencies responding to requests for information indicated that much of the information on intrusion detection devices has been designated as classified defense information. Such information can only be released to firms and/or persons on a "need to know" basis. It appears that firms operating under Federal Government Industrial Security programs could obtain this information by applying through their cognizant security officer. Even if this information were available, it could not be presented in this study.

---

[10]Mosler Research Products, Incorporated, "Electronic Anti-Intrusion Systems and Electronic Investigative Equipment" (Danbury, Connecticut: Mosler Research Products, undated).

CHAPTER III

INTRUSION DETECTION SYSTEMS

In order to understand intrusion alarm systems, it is necessary to know something of the development of the alarm industry; components of a modern intrusion detection system; principles of their operation; field applications of such equipment; recent developments in intrusion alarm equipment; and the role of Underwriters' Laboratories. These areas will be the focus of the present chapter.

I. HISTORY AND DEVELOPMENT OF THE INTRUSION ALARM INDUSTRY

One might have the impression that electric intrusion alarms are a product of the twentieth century. This is not the case. The first electric burglar alarm was patented in 1853 soon after a suitable battery was developed to supply the necessary electrical current.[1] They were first called burglar alarms because they were designed and installed in homes and places of business to protect them from burglary. The early alarms were of the local alarm variety; that is, when an intruder caused an alarm, a gong or other noise producing device was activated to alert

---

[1]Blake Clark, "Bad News for Burglars," Banking, VL (June, 1953), 120.

policemen or other persons in the immediate vicinity. This type of protection is still found in some of the older banks in this country as indicated by the presence of bell housings on exterior walls.

As early as 1858 telegraph companies were established which provided a burglar alarm service.[2] They were called district telegraph companies because the cities in which they were located were divided into districts with an office in the center. The size of the district was conditioned by the distance that a messenger could run in three minutes. Instruments installed in homes or places of business were connected by telegraph wires to the central office in the district. By turning one of three levers it was possible to summon a policeman, fireman, or messenger boy. If a burglar broke into the home or place of business a lever could be pushed and a telegraph company guard would soon appear. If a fire was discovered, the subscriber simply pushed another lever and a fireman was immediately notified. If the subscriber wanted to send a message, the third lever was pushed and within three minutes a messenger boy would arrive.

The instrument also had an attachment which could be connected while the subscriber was absent from the premises. If an intruder entered the area an alarm would be

---

[2]Edward H. Smith, "The Burglar and the Alarm," Scientific American, CXVIII (May, 1923), 294.

sounded in the central station and a company guard would be dispatched to investigate. The instrument of each subscriber caused a distinctive alarm so personnel at the central station were able to determine immediately the source of the alarm and dispatch guards to the proper location.[3]

The electrical alarm also served as an effective deterrent to burglary due to the general lack of knowledge and consequential mystery surrounding electricity. In most cases burglars would not take the risk of entering electrically protected property and would attack unprotected property instead.[4]

Early in the twentieth century, district telegraph companies lost most of their popularity due to increased use of the telephone. During this period fifty-seven of the smaller telegraph companies merged to form the American District Telegraph Company, which has developed into the world's largest protection company.[5]

Early burglar alarms consisted of simple electrical switches on doors, windows, and other openings. The first systems employed an open circuit connection which could be defeated by simply cutting any of the wires in the circuit. A closed circuit connection was soon adopted which

---

[3]"The Domestic Telegraph," Scientific American, XXVII (July 20, 1872), 39.

[4]"Safeguards for Jewelers," Detector (March-April, 1960), pages unnumbered.

[5]Ibid.

would sound an alarm if one of the wires was severed.

From 1857 to 1925 there were no significant changes in intrusion alarm equipment. New types of equipment were not developed and the only changes involved improvement of existing types.

In 1925 an audio alarm was invented. The principal component of this system was a sensitive microphone which was installed in a bank vault or other secured area. When intruders attempted to break into the area the noise of the intrusion was picked up by the microphone and initiated an alarm.[6]

In 1935 a photoelectric alarm device was developed. This device consisted of a light source and a receiver containing a photoelectric cell. A light beam was projected between the light source and receiver and any interruption of the beam caused an alarm.[7]

Around 1940 a capacitance alarm was invented which surrounded a protected object with an electromagnetic field. When anything solid touched or came close to the protected object the electromagnetic field was disrupted and an alarm was sounded.[8]

In 1952 a sound wave alarm was introduced. The

---

[6]"Loudspeaker Burglar Alarm," Science Newsletter, LXXXIII (March 20, 1936), sup. 9.

[7]"Safeguards for Jewelers," Detector (March-April, 1960), pages unnumbered.

[8]Ibid.

principal components of that alarm were a sound wave transmitter which emitted a high frequency sound wave into an enclosed, protected area, and a receiver which picked up the sound waves after they had been deflected by the walls, ceiling, floor, and objects in the room. Any movement in the enclosure changed the sound wave pattern and initiated an alarm.[9]

These are the systems which are in common use today for both mercantile and industrial plant protection. Each of these will be discussed in detail in a later part of this chapter.

As indicated, the early alarms were designed and installed for the purpose of preventing burglary. It is easy to understand the reason for the use of the term "burglar alarm" as a generic description of all systems installed to guard against loss of cash or other valuable property by breaking and entering unoccupied areas. A need for such devices was most acutely felt in the commercial and mercantile field, particularly banks and other financial institutions. It became apparent that adequate security could not be provided by full time guards due to the prohibitive costs. It was also obvious that physical barriers alone could not stop a determined thief. These firms turned to electric alarm systems to provide dependable but relatively

---

[9]Stanley Kempter, "Ultrasonic System Detects Intruders," Electronics, XXV (April, 1952), 104.

inexpensive protection. For many years this was the only purpose served by intrusion alarms.

During World War I sabotage by German agents caused damage of $150,000,000 in the United States.[10] In order to prevent similar losses in World War II industrial and government facilities turned to alarm devices to improve security. This greatly increased the demand for adequate alarm systems.[11] Intrusion alarms were used to augment available security guard personnel. This wartime situation provided the stimulus which resulted in the development of improved alarm systems during this period. As a result of this new role, alarms took on the new title of "intrusion detection alarms" or "security alarms." It was necessary that alarms designed for this purpose be more reliable than alarms previously used to prevent burglary. The trained enemy agent could be expected to have more technical knowledge and skill than the average burglar.

After World War II as the international situation began to crystallize into the "cold war" atmosphere, it became obvious that continuation of strict security measures would be necessary. This situation, of course, had a direct influence on the intrusion alarm industry and

---

[10] "Robot Guardians of Billions," Popular Mechanics, LXXXIX (February, 1943), 28.

[11] Mosler Research Products, Incorporated, "Electronic Anti-Intrusion Systems and Electronic Investigative Equipment" (Danbury, Connecticut: Mosler Research Products, undated), p. 1.

alarm research continued. Federal Government Industrial Security programs, which required firms with classified government contracts to meet certain minimum security standards, greatly increased the sale and use of intrusion alarms. In 1957 it was estimated that 60% of all electronic alarm systems were installed at plants working on classified projects.[12]

In addition to the necessity to secure industrial facilities, it was necessary to provide protection for military storage and operational installations which were required for defense and retaliation in case of enemy attack.

Another reason for the expansion of the industry was increased competition between firms of the free world after World War II. This caused firms to establish security measures to keep "trade secrets" and "industrial know-how" out of the hands of their competitors.

The rising crime rate was another reason for the expansion of the alarm industry. Each year the number of burglaries and resulting monetary loss from such attacks seemed to rise. During the period 1951 to 1961 the total number of burglaries--breaking and entering--rose from 407,130[13] to 852,500 annually.[14] This includes both homes

---

[12]"Intruder Alarm Market Up," Electronics, XXX (April 10, 1957), 30.

[13]Federal Bureau of Investigation, Uniform Crime Reports--1951 (Washington: Government Printing Office, 1952), p. 70.

[14]Federal Bureau of Investigation, Uniform Crime Reports--1961 (Washington: Government Printing Office, 1962), p. 2.

and commercial facilities. Today the central station alarm industry is composed of more than 100 different companies which service approximately 150,000 subscribers in over 2,000 different cities. The number of subscribers increased approximately 50% during the period from 1949[15] to 1961.[16] In 1960 the American District Telegraph Company alone had over 100 central stations in all parts of the United States and was serving 70,000 subscribers.[17] This included industrial, mercantile, and private dwelling installations but did not include proprietary systems not serviced by central stations. In 1961 the central station alarm industry protected about 70 billion dollars worth of property and billions of dollars in cash and securities. These firms usually install and maintain the alarm equipment and provide guards that respond to alarm signals received at the central station. The total capital investment of the industry in 1961 was 157.4 million dollars and earned revenue was estimated at 74.5 million dollars during the same year.[18] These figures give some indication of the present size of the alarm industry.

---

[15]Department of Commerce, Business Outlook for 1960 (Washington: Government Printing Office, 1959), p. 29.

[16]Department of Commerce, Business Outlook for 1962 (Washington: Government Printing Office, 1961), p. 35.

[17]"Safeguards for Jewelers," Detector (March-April, 1960), pages unnumbered.

[18]Department of Commerce, Business Outlook for 1962, loc. cit.

Some alarm manufacturers devote their entire efforts to research, development, and production of alarm systems for the protection of critical military and industrial facilities which are vital to national defense. Most manufacturers, however, produce equipment which is used for the prevention of theft as well as protection of classified information.

II. ALARM SYSTEM COMPONENTS

There are two alarm connection systems which are most frequently used in industrial plant protection. The first is the central station system, in which the alarm is connected to an alarm panel in a central station; when an alarm is received the company, which is usually privately owned, dispatches one of its guards and/or police officers to investigate. The second is the proprietary system which is very similar to the central station system except that the alarm panel is located in a guard room maintained by the owner of the protected property and the firm's own guards respond to alarms. Firms large enough to justify a full time guard force normally use the proprietary system. Since many industrial plants are in this category, the latter system is often used.

In either case the components of the system are basically the same. Both the proprietary and central station systems in common use today consist of three basic

components: (1) A sensing system located in the protected area which detects intrusion and initiates an alarm; (2) monitoring equipment located in a guard room or central station which gives a signal when an alarm is received; and (3) connecting signal wires which electrically connect the other two components. These components and their principles of operation and field applications will be discussed in detail in this section of the study.

Sensing System

The sensing system is the portion of an intrusion alarm system which detects intrusion into a protected area and initiates an alarm signal. The system is composed of one or more detectors (detection devices) which are activated by breaking an electrical circuit, sound, interruption of a light beam, disruption of an electromagnetic field, or movement. The detectors that make up the system are normally connected by wires with a control unit in the protected area which serves to integrate the various detectors into a sensing system. The control unit contains the necessary equipment to receive impulses from the devices and transmit an alarm signal over the signal wires to the monitoring equipment. There are five types of detection devices in general use today: electromechanical, audio, photoelectric, capacitance, and sound wave. A sensing system may be composed of one, or a combination of different type detection devices.

Electromechanical Detectors. This is the oldest and simplest type of detection device in common use. Due to its simplicity, it is also probably the easiest type to breach.[19] In many security systems they are used only to supplement other primary detection devices.

They are normally connected into a continuous wired circuit that carries an electrical current. When an intrusion is attempted this circuit is broken and an alarm signal is initiated. Although generally used to protect openings such as doors and windows, they may also be used to protect walls, floors, and ceilings.

There are many types of electromechanical devices, but the principle of operation is basically the same. As the name implies, they are activated by some mechanical action which interrupts an established electrical circuit and causes an alarm.

The most common type electromechanical detection device is a mechanical switch which is used on doors and windows. These devices are attached in such a manner that opening the door or window opens the switch and breaks the circuit, causing an alarm.[20]

Metallic foil is used for the protection of windows

---

[19]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961), p. 13.

[20]Ibid., p. 14.

and glass door panels. Strips of foil which carry current are attached directly to the glass with a special adhesive. It is attached in such a manner that the tape is broken if the glass is smashed. A foil system is somewhat prone to false alarms[21] and may be easily bypassed by connecting a jumper wire across terminal points of the foil. The Army Ordnance Corps does not consider this device suitable for use in military security installations under their control.[22]

Wire trap detection devices are used to protect skylights and other similar openings. This device consists of two layers of thin wires running across the opening. Each layer is run at right angles to the other and the layers are less than six inches apart. The wire trap may be removable to permit cleaning of windows or they may be permanently attached to the building. In order to prevent bridging a double circuit system is used.[23] Breaking or grounding one of the wires causes an alarm.

Screen type detection devices are prepared by cementing small wires in wooden dowels and installing the dowels in openings. The enclosed wires are connected to

---

[21]Minneapolis-Honeywell Company, Security and Equipment Surveillance Systems (Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated), p. 11.

[22]Department of Army, Intrusion Detection Systems, ORDM 10-2, op. cit., p. 15.

[23]Underwriters' Laboratories, Standards for Safety; Installation, Classification and Certification of Burglar Alarm Systems, UL 681 (Chicago: Underwriters' Laboratories, 1959), p. 14.

form a continuous circuit which is interrupted if one of the dowels is broken.[24]

One manufacturer produces an electromechanical device which is activated by pressure on a taut wire. A spring tempered wire is pulled taut to approximately twelve pounds pressure along the top of a fence. A force of three to twelve pounds (adjustable) applied to the wire trips a microswitch and causes an alarm. One detector panel containing necessary contacts can handle 400 feet of wire.[25] The device is based on the assumption that a person climbing a protected fence would place his hand on top of the fence in order to climb over and thus put pressure on the wire and cause an alarm. It appears that if an intruder knew the fence was protected it would be easy to climb the fence without touching the wire and causing an alarm.

Another type of detection device that may be placed in the electromechanical category is the vibration detector. This device is normally used to supplement other detection devices. It protects against attack through walls, ceilings, and extensive glass surfaces. The device contains a small pendulum-like weight which in its normal position maintains a closed circuit. An attack on the surface upon

---

[24]Department of Army, Intrusion Detection Systems, ORDM 10-2, op. cit., p. 15.

[25]Minneapolis-Honeywell Company, Taut Wire Detector (Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated), pp. 1-2.

which it is mounted causes vibrations which moves the pendulum, opening the circuit, and causing an alarm.[26]

One electromechanical device uses a feeble vacuum that is produced by a small exhaust fan installed in the wall of the protected vault or structure. A very sensitive diaphragm in the protected structure detects any change in air pressure and causes an alarm. The pressure change could be produced by opening a door, or breaching the floor, ceiling, or one of the walls.[27] Even a small hand hole would be sufficient to cause an alarm.[28]

One common criticism of electromechanical detection devices is that they offer no protection against the "stay behind" intruder. This type of intruder hides in an area during normal business hours and after closing time takes what he wants and smashes his way out. In a protected area this exit causes an alarm but the intruder is generally able to escape before the police or guards arrive. In order to provide some protection against this type of operator a "floor trap" detection device was developed. This device is put into service by stretching thin wires around the protected premises, keeping them close to the floor.

---

[26]American District Telegraph Company, Protecting Life, Property, and Profits (New York: American District Telegraph Company, 1959), p. 30.

[27]"At Home: No Unauthorized Entry," Engineering, CXCIII (January, 1962), 120.

[28]Philip Gustafson, "These Safecrackers Can Get Away with It," Popular Science, CLIII (March, 1948), 117.

Plugs at each end of the wire are fitted into sockets on the walls, completing an electrical circuit. As the intruder moves around, usually in the dark, he causes an alarm if one of the wires is cut or pulled out of the sockets.[29]

Heat detectors and bolt protectors are special purpose electromechanical devices which are used to supplement primary protection on safes and vaults. The heat detector which contains a pneumatic switch causes an alarm if heat is applied to the safe or vault door. The bolt protector is installed on bolts in safe and vault doors and causes an alarm if one of the protected bolts is turned or otherwise tampered with.[30]

There are several other "custom" adaptations of electromechanical devices. Walls and ceilings are sometimes protected by wiring run through wooden dowels installed in them. Walls and ceilings may also be protected with plywood or wallboard which contains inner electrical conductors. Floors and walls can also be protected by installing electrical cable in concrete.[31]

Electromechanical devices must generally be used

---

[29]Robert Gorman, "War Between Burglars and Inventors," Popular Science, CLXXVI (April, 1960), 94.

[30]American District Telegraph Company, Electric Protection Services, Book II (New York: American District Telegraph Company, 1960), p. G6-9.

[31]John R. Davis, Industrial Plant Protection (Springfield, Illinois: Charles C. Thomas, Publisher, 1957), p. 123.

to supplement other detection devices. When used alone they provide a relatively low level of security. When the devices are used only to secure openings it is possible to break through walls, ceilings, and floors without causing an alarm. The devices are relatively inexpensive and installation accounts for most of the cost involved. For this reason such a system is not flexible since the equipment has little salvage value and cannot be easily moved when security requirements change. The devices can, however, provide inexpensive supplemental protection for rooms with a few small openings.[32]

Audio Detectors. Audio detection devices are used to protect most of the nation's bank vaults. When properly installed and supplemented by other basic detectors such as heat detectors and bolt protectors, they provide the highest grade of alarm protection recognized by Underwriters' Laboratories.[33] An indication of their effectiveness is the fact that of 15,000 such approved installations in bank vaults there was not a single loss during a ten year period.[34]

The principal components of audio detectors are a sensitive microphone and an amplifier which are both

---

[32]Mosler Research Products, Incorporated, op. cit., p. 2.

[33]Powers Regulator Company, Introduction to Security Systems (Skokie, Illinois: Powers Regulator Company, 1961), p. 7.

[34]"Robot Guardians of Billions," Popular Mechanics, LXXIX (February, 1943), 177.

installed in the protected area. The microphone is sensitive to all sounds within the audible range but is generally designed to give peak response to those frequencies which might result from an attack on the protected enclosure.[35] For this reason this detection device is best suited for vaults or other areas which are relatively soundproof and require a reasonable amount of force to breach. The noise incident to forcible entry into the structure is picked up by the microphone, causing a change in an electrical circuit, thus initiating an alarm.[36]

It is necessary to adjust the sensitivity of the device so ambient or normal noises will not cause an alarm. After this adjustment is made, noises above this level will be amplified with enough power to activate the alarm relay in the control unit.[37] In order to determine if the detectors are sensitive enough, representatives of Underwriters' Laboratories, in conducting their inspections of installed alarm systems, use a recording which was made of an actual forcible intrusion into a vault. The recording was made at the laboratories and is played in the protected area to determine if it will cause an alarm.[38]

---

[35]American District Telegraph Company, Electric Protection Services, Book II (New York: American District Telegraph, 1960), p. E2-7.

[36]Ibid.

[37]Powers Regulator Company, op. cit., p. 6.

[38]Philip Gustafson, "These Safecrackers Can Get Away with It," Popular Science, CLII (March, 1948), 114.

Some audio devices require sound test and power units as accessory equipment. The sound test unit is simply a horn which is activated from the guard headquarters or central station to test the detectors. The power for the detectors is supplied from a central location but the power unit is required to operate the sound test unit.[39]

One type sensing system which employs audio detectors also includes a preamplifier which is installed so the guard at a central location can throw a switch and convert the system to a listening device. This enables him to listen for sounds in the protected area which might indicate the presence of intruders. He is able to dispatch guards to investigate and continue to monitor while they are enroute in order to obtain additional information on the intruder's activities. This information can then be relayed to the investigating patrol by radio or other means of communication. He may be able to establish definitely the fact that an intrusion has been made or the number of men involved which would enable the guards better to cope with the situation.[40]

As indicated earlier, the greatest potential problem in using audio detectors is false or nuisance alarms

---

[39]American District Telegraph Company, op. cit., p. #2-9.

[40]Minneapolis-Honeywell Company, Security and Equipment Surveillance Systems (Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated), p. 14.

caused by thunder, truck backfires, or other common noises. One alarm manufacturer uses an electronic discriminator panel which it claims will eliminate such nuisance alarms. Another possible solution is the use of "contact" microphones. These are installed on the inside walls of a vault or other protected area and will detect sound vibrations through a thick wall but will not respond to airborne noises.[41] This type detector may also be used to protect soft, easily penetrated walls.[42]

Prior to installation of audio detectors a careful study of the area is mandatory. Noises which are not noticeable to a casual observer may result in an excessive number of nuisance alarms or necessitate reduction of sensitivity, thus reducing the protection provided. Noises caused by telephones, furnaces, water coolers, radiators, or other normal equipment may make use of the equipment impractical. This problem was encountered in the Library of Congress where the noise made by rats was sufficient to cause nuisance alarms.[43] Outside noises caused by trains, whistles, or automobile traffic may also produce false alarms. Structures best suited for audio detection devices are those of masonry or similar construction, or other non-sound absorbent

---

[41] Ibid.

[42] Powers Regulator Company, op. cit., p. 7.

[43] Robert Gorman, "War Between Burglars and Inventors," Popular Science, CLXXVI (April, 1960), 223.

material.[44]

Careful study is also necessary to determine the number and sensitivity of detectors. This is made more complex if the area contains a large amount of sound absorbent material or if the amount of material stored in a protected area varies significantly.[45]

The audio detector is easily installed, relatively inexpensive, has a high salvage value, and may be easily removed and reinstalled if the security requirement changes. Two of the disadvantages to use of the equipment are that its sensitivity to all audible sounds restricts its range of application; and some models which use vacuum tubes require frequent sensitivity checks. The latter has been overcome in some models through use of transistorized circuitry.[46]

Photoelectric Detectors. The photoelectric detection device is similar to the familiar photoelectric system used to open doors automatically at supermarkets.[47] The principal components of such devices are: a projector, a

---

[44]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961), p. 7.

[45]American District Telegraph Company, op. cit., p. E2-7.

[46]Powers Regulator Company, op. cit., p. 7.

[47]"Automate Plant Protection," Factory, CXIX (December, 1961), 62.

light sensitive receiver, and a control unit.

The projector generally consists of one or more incandescent electric lamps, a lens and filter system; and, in some models, a motor driven perforated disc. The electric lamps provide the necessary light which is projected through, and controlled by, the lens. In some models two lamps are used to double the light intensity, and to provide continuous protection if one lamp fails.[48] A filter is used in all security devices to eliminate light in the visible spectrum so the projected beam cannot be seen, and thus avoided, by an intruder.

In order to prevent the introduction of a substitute light source, the light beam is generally modulated. In some cases this is accomplished by introducing a motor driven perforated disc between the light source and the receiver. As the disc rotates it interrupts the light beam at a given frequency. The receiver is synchronized to this same frequency and is thus unaffected by other light maliciously or accidentally introduced. When this motor driven disc is used it is a part of the projector unit.

A more recent device modulates the light electronically through use of a transistorized unit which is less expensive and has a higher life expectancy than the motor

---

[48]Maxwell Lindsay, "Electronic Protective Systems," Electrical Engineering, LXIII (October, 1944), 369.

driven modulator.[49] The modulated frequency produced by the electronic unit is made slightly different from normal alternating current frequency so an intruder cannot defeat the detector with a sixty cycles per second strobescope.[50]

The light receiver contains a photoelectric cell which converts light energy to electrical energy. As long as light is received at the cell in the proper frequency, a continuous circuit is maintained. If the light beam is interrupted, the circuit is broken and an alarm is initiated. Thus an intruder passing between the projector and receiver causes an alarm.[51]

The control unit required for operation of this type detector contains equipment to supervise the circuit, receive signals from the photoelectric detectors, and transmit an alarm signal to the master sensing system control unit. If other detector types are not used, the photoelectric control unit can transmit signals directly to the guard room or central station.[52]

There is one other photoelectric detector which

---

[49]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961), 11.

[50]Sam Bagno and J. Fasal, "Intruder Alarm Uses Phase-Sensitive Detector," Electronics, XXXI (February 14, 1958), 102.

[51]Department of Army, loc. cit.

[52]American District Telegraph Company, Electrical Protective Services, Book II (New York: American District Telegraph Company, 1960), p. E5-10.

uses a different principle of operation. This device is operated by change of light intensity reflected from an independent light source. The light source is not electrically connected with the receiver which operates like a light meter. As long as the light from the light source remains constant a closed circuit is maintained. If an intruder enters the area, this changes the amount of reflected light received at the "light meter" and causes an alarm. This device is less restrictive in its application than the conventional photoelectric detector since it provides area protection. If an intruder approaches the device in an attempt to tamper with it, an alarm signal is initiated. It is generally more expensive than other detectors which provide the same type protection.[53]

Since the light beam projected by a photoelectric detector is generally narrow and travels in a straight line, it may be easily by-passed if an intruder knows of its presence. For this reason the components of the device should be concealed whenever possible. One manufacturer produces a miniature device which is installed in the wall and resembles a standard light switch.[54]

Another method of increasing the effectiveness of

---

[53]Department of Army, Intrusion Detection Systems, ORDM 10-2, op. cit., p. 13.

[54]Worner Electronic Devices, Fotoelectric Systems (Rankin, Illinois: Worner Electronic Devices, 1962), p. 22.

photoelectric detectors is through the use of mirrors. Mirrors, however, reduce the linear capability of the detector by about fifty per cent each time a mirror is used. Better detectors have an eight hundred foot inside range limitation and this is cut in half each time a mirror is introduced.[55] With mirrors it is possible to provide a protective perimeter around an area or interlace a room with beams to provide some protection from a "stay behind" intruder. Photoelectric devices with mirrors are often combined with electromechanical devices for better coverage of a secured area against penetration of unprotected walls and ceilings. They may also be used to protect long rows of windows in lieu of metallic foil or other electromechanical devices. This is accomplished by deflecting light beams back and forth across the area with mirrors. Lenses and mirrors, if used, must be kept clean at all times in order for the equipment to operate properly. Precautions must also be taken to insure that mirrors are in proper alignment.[56]

Photoelectric devices are sometimes used outdoors to protect perimeter gaps, gates, roadways, aircraft runways, harbors, or other areas where physical barriers cannot

---

[55]American District Telegraph Company, op. cit., p. E4-7.

[56]Powers Regulator Company, op. cit., p. 6.

be used.[57] Its use outdoors is restricted, however, due to the limitations imposed by weather conditions, vulnerability to defeat, and susceptibility to alarms initiated by natural causes. Any interruption of the light beam by snow, rain, fog, or miscellaneous debris, will cause a nuisance alarm.[58] For outdoor use the terrain must be relatively level. Rough terrain makes its use impractical due to the number of devices required to conform to ground contours.[59] The equipment must also be mounted on a solid foundation or shifting will disturb alignment.

Photoelectric devices generally have a high salvage value and can be easily relocated if security requirements change. In some cases the equipment supplements ordinary fire protection equipment. When smoke becomes dense enough to interrupt the light beam, an alarm is initiated.

One disadvantage of the device is that it operates on one hundred and ten volt current and normally requires a standby power source for emergency operation. Another disadvantage is the fact that models which use vacuum tubes require frequent checks. More modern equipment uses transistorized circuitry.[60]

---

[57]Mosler Research Products, Incorporated, op. cit., p. 6.

[58]Department of Army, Intrusion Detection Systems, CRDM 10-2, op. cit., p. 13.

[59]American District Telegraph Company, op. cit., p. E5-9.

[60]Mosler Research Products, op. cit., p. 6.

Capacitance Detectors. Capacitance devices detect intrusion by establishing an electromagnetic field around the object to be protected. The approach of an intruder or introduction of other foreign objects into this field initiates an alarm.[61] This phenomenon can be demonstrated by touching or placing a hand near the "rabbit ears" of a conventional home television set. The antenna establishes an electromagnetic field similar to the capacitance detector and a human hand disrupts the field, causing a change in the television picture.[62]

The capacitance device is generally used for point protection of file cabinets, safes, and other similar metallic objects which can be insulated from the ground. It may, however, be used for protection of ceilings, walls, doors, and windows. The principal components of this detector are a control unit and one or more protected objects or antennae.

The control unit contains circuitry which is capable of generating the electrical field which is established around the protected object or antennae; detecting a rapid change in capacitance between the antennae and the ground; and initiating an alarm. If other detector types are

---

[61]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961), p. 16.

[62]Minneapolis-Honeywell Company, Secret Sentry, W614 (Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated), p. 1.

employed in the same area, this control unit may be connected to a master sensing system control unit. If other devices are not used in the same area, the detector control unit can transmit an alarm signal directly to guard headquarters or a central station. Since changes in temperature and humidity, as well as intrusion, change capacitance, the control unit is designed to compensate for such gradual changes without causing an alarm.

The control unit is electrically connected to one or more antennae which in many cases is the protected object itself. Since the detector is operated by a change in capacitance between the antenna and ground, it is necessary to insulate the protected object or antenna from ground to prevent leakage of electrical energy.[63] In the case of safes, filing cabinets, and similar objects, this is accomplished by placing them on non-conductive insulator blocks.

When the protected object or antenna is charged it acts as one plate of a condenser with the surrounding walls, floor, and other objects serving as the opposite plate; the air in between them serves as an insulator. The presence of an intruder or other object causes a capacitance change sufficient to be detected by the detector

---

[63]Thomas J. Murphy, "The Capacity Alarm Comes of Age," Signal, VI (February, 1960), 8.

control unit and initiates an alarm.[64]

The electromagnetic field that is established normally extends only a few inches but can be extended to several feet. This is not normally done, however, because it would only serve to give an alarm one or two seconds earlier and would result in accidental alarms caused by persons approaching the object with no intent of intrusion. Janitors and other maintenance personnel could cause alarms by cleaning near the protected object. There have also been cases where the electromagnetic protective field extended through walls which were not properly shielded and alarms resulted from persons standing near an outside wall.[65]

This detector may also be used to protect walls, ceilings, and floors, by installing antenna wires on or in them. Openings may also be protected by installing metal antenna grids or wires over the openings. One device employs a single antenna wire which is run inside a wall and over doors so passage through a door or an attempt to breach the wall would cause an alarm.[66] In such an installation it appears that persons using adjacent rooms and passages would also initiate alarms.

---

[64]Mosler Research Products, Incorporated, op. cit., p. 10.

[65]"Robot Guardians of Billions," Popular Mechanics, LXXXIX (February, 1943), 31.

[66]Minneapolis-Honeywell Company, Secret Sentry, W614, op. cit., p. 1.

Through use of transistorized circuitry it is possible to operate this detector without a normal alternating current power source. This permits a great deal of flexibility and they can be used in trucks, trailers, and similar vehicles.[67]

Since the equipment for this detector is usually compact and inconspicuous it is difficult for intruders to determine which objects are protected so they do not know when an alarm has been initiated.

The equipment has a high salvage value and is simple to install and operate so it can be easily moved if security requirements change.

The detector cannot be used on ungrounded equipment and it is necessary to keep the area surrounding the protected object free from foreign objects that might affect the electromagnetic field.[68]

The electronic fence or electromagnetic fence is another type detection device which is very similar to the capacitance detector and was included under this heading for this reason. Some firms use the capacitance device to provide outside perimeter protection but other firms employ the electronic fence which uses a slightly different principle to provide such protection. This fence is generally

---

[67]Mosler Research Products, Incorporated, op. cit., p. 11.

[68]Ibid.

used to provide perimeter protection for storage areas, industrial property, classified military installations, and similar areas. It may also be used to protect building exteriors, and windows and other possible points of entry into buildings.

The principal components of this detector are a control unit and transmitting and receiving antennae. The control unit contains circuits which generate a low frequency electromagnetic signal which is transmitted in all directions by the transmission antenna. Two or more receiving antennae which are placed parallel to and in the same field as the transmission antenna receive the emitted signal. The energy picked up by the receiving antennae is relayed to a supervisory circuit in the control unit. If a person or object enters the electromagnetic field established between and around the antennae, it affects the amount of energy received, which is detected by the supervisory circuit and an alarm is initiated.[69]

For outside perimeter protection the antennae are installed on existing chain link fence or their own supporting posts. The perimeter is generally divided into zones of approximately two-hundred feet in order to facilitate the identification of intrusion attempts.[70]

---

[69]Powers Regulator Company, AL-15 Radi-Matic Barrier (Skokie, Illinois: Powers Regulator Company, 1961), p. 1-2.

[70]Mosler Research Products, Incorporated, op. cit., p. 12.

It is claimed that this detector will not emit radiation which might interfere with nearby communications equipment and in turn is not disturbed by broadcasting, short wave transmissions, magnetic storms, etc.[71]

At normal settings the system will detect intrusions within three to four feet of one of the antennae wires but it can extend this field up to eight feet.[72]

By installing the antennae on the face of buildings, or over windows or other possible points of entry, this device can also provide protection for warehouses or other buildings.

One of the principal advantages of this device for perimeter protection is that it gives early warning of intrusion before access is made to more critical areas, thus providing protection in depth. It can also be used to protect goods which are in open storage and cannot be otherwise secured.[73]

Some disadvantages of the device are that the area adjacent to the antennae must be cleared and be kept free of weeds and other debris. It is also mandatory that the electronic fence be inside another fence or barrier to prevent alarms caused by casual intruders or animals.

---

[71] "Safe as a Bank Vault," Factory, CXIV (June, 1956), 95.

[72] Ibid.

[73] Powers Regulator Company, Introduction to Security Systems (Skokie, Illinois: Powers Regulator Company, 1961), p. 11.

Sound Wave Detectors. Sound wave detection devices use the Doppler effect to detect motion in a confined protected area. The phenomenon of the Doppler effect can be observed by standing near a railroad crossing as a locomotive passes with its whistle blowing. As the train approaches the crossing there is a rising pitch to the sound of the whistle and as it passes, the tone of the whistle drops abruptly. As it approaches, each sound wave produced by the whistle is emitted from a point nearer the crossing than the previous one. This causes each wave to reach the observer's ear sooner than it would if the whistle were in a fixed position. As a result, more sound waves strike the ear as the train approaches, causing a rise in the tone of the whistle. The opposite is true as the train departs and results in a falling tone. It has also been shown that similar results are obtained when the receiver (or observer) is moved toward or away from a stationary sound source. Further study proved that even when the sound source and receiver were both fixed, the echo pattern produced from sound waves reflected from a moving object in the vicinity is different from the pattern produced by waves striking a stationary object. This same principle is used in the operation of sound wave detectors.[74]

---

[74]Walter Kidde and Company, Incorporated, Kidde Ultrasonic Alarm Systems (Clifton, New Jersey: Walter Kidde and Company, Incorporated, 1962), p. 4.

The principal components of a sound wave detector are a transmitter, receiver, and detector control unit. The transmitter emits sound waves which saturate the protected area. As these waves are deflected from the walls, ceiling, floor, and other objects in the room, a definite echo pattern is established. The receiver, acting as a microphone, picks up the sound waves either directly from the transmitter, or after being reflected from objects in the protected area. Since every solid object in the area produces an echo, any movement causes a change in the pitch of the echo pattern due to the Doppler effect. This change disrupts the previously established pattern and is used to initiate an alarm.[75]

The control unit is electrically connected to the transmitter and receiver components and has been called the "electronic brain" of the detector.[76] It consists of a constant-voltage power transformer to reduce line current, an oscillator to create the sound wave, and other components to receive and amplify alarm signals.[77] This "brain" monitors the echo pattern which is established in the protected area and is able to detect any slight change in the pattern

---

[75]Sam Bagno, J. B. Cooper, and E. I. Levy, "The Ultrasonic Burglar System," IRE Convention Record, part 6, Audio and Ultrasonics (New York: Institute of Radio Engineers, 1954), p. 49.

[76]Walter Kidde and Company, Incorporated, op. cit., p. 5.

[77]American District Telegraph Company, Electric Protection Services, Book II (New York: American District Telegraph Company, 1960), p. E4-12.

caused by movement. When this change is detected the unit sends an electrical signal over the signal wires to the guard room or central station. If other types of detectors are used in the same area the signal may be transmitted through a master sensing system control unit which integrates all types of detectors in the area. The detector control unit has a sensitive adjustment which can be tuned to compensate for temperature changes, small animals, air currents, or other disturbing factors.[78] In a room with a ceiling height of less than 15 feet, one transmitter and receiver connected to the control unit can provide protection for an area of approximately one thousand square feet.[79] The exact coverage will depend upon the contents of the room and the accoustical characteristics of the walls, floor, and ceiling.[80] Some control unit models provide protection for four thousand square feet by controlling four transmitters and receivers. One model can be modified to control twenty-four transmitters and receivers by addition of an optional power amplifier.[81]

There are two types of sound wave detectors in general use today. One uses a sound frequency above the normal

---

[78]Walter Kidde and Company, op. cit., pp. 5-6.

[79]American District Telegraph Company, op. cit., p. E4-12.

[80]Stanley Kempner, "Ultrasonic System Detects Intruders," Electronics, XXV (April, 1952), 105.

[81]Walter Kidde and Company, op. cit., p. 7.

audible range of the human ear and the other uses an operating frequency which is audible to humans (below 18,000 cycles per second). The higher frequency detector is commonly called "ultrasonic" due to the high frequency employed (generally around 19,200 cycles per second).[82] The principle of operation of the two is basically the same.

In addition to the difference in frequency, the two detection devices differ in external appearance. The "ultrasonic" transmitter and receiver have been described as "two units about the size of half a softball."[83] These units or domes are mounted at different locations about ten feet above the floor; one contains a transmitter and the other a receiver. This type detector is also available in a completely portable model which fits into a custom made carrying case and permits easy movement to areas where temporary protection is desired. One large manufacturer keeps an extra portable set on hand to provide temporary protection whenever it is needed.[84] The "ultrasonic" detector is normally equipped with a small motor-driven vane built into the transmitter which is used to test the device from the guard room or central station. When the vane is

---

[82]"Ultrasonic Alarm: Alertonic," Time, LXII (October 26, 1953), 91.

[83]"How Dayton Minimizes Vandalism Losses," American School Board Journal, CXL (May, 1960), 48.

[84]Walter Kidde and Company, op. cit., p. 10.

activated it breaks up the sound wave pattern and produces a test alarm.[85] If this testing device is not available a "walk test" can be used in the protected area. Another bonus derived from the use of "ultrasonic" detectors is that it will rid the premises of mice and other rodents. It is claimed that the sound waves, which are inaudible to humans, cause discomfort to the rodents and cause them to move to a new location. This same characteristic would also preclude the use of dogs in the protected area.[86]

The transmitter/receiver for the lower frequency system is similar to a standard loudspeaker in appearance and operation. Both the transmitter and receiver are contained in this single unit. Limited area coverage can be provided by orienting the unit toward the area to be protected. Complete coverage of an enclosed area can be provided by using two or more of the units placed in opposing locations such as opposite walls of a protected room. At one time, this type detector caused a high pitched whine which could be distracting to personnel in the area; in later models the volume and intensity were reduced without reducing the effectiveness of the device. The lower frequency system is also less likely to cause nuisance alarms due to disturbing factors such as air currents and changes

---

[85]Kempner, op. cit., p. 105.

[86]U.S. Army Intelligence School, Electrical Protective Systems; Supplemental Reading Number 30612 (Fort Holabird, Maryland: U.S. Army Intelligence School, 1962), p. 8.

in temperature.[87]

When sound wave detectors are used it is desirable that all objects in the protected area be stationary except the one that is to be detected. This is seldom possible so it will generally be necessary to reduce the sensitivity of the detector to compensate for slight movement of objects such as window curtains. As mentioned earlier, this is easily accomplished by adjustment of the control unit; it should be kept in mind, however, that reduction of sensitivity may also reduce the effectiveness of the system.

Another disturbing effect that must be considered is turbulence of air currents in the protected area. The turbulence caused by convection or other currents of air may have an appreciable effect on the detection device. As sound waves travel through a moving current of air, the speed of the waves is altered and this tends to disrupt the echo pattern established by the device.[88]

Temperature also has an effect on the operation of a sound wave detector. A change in the temperature of the air in the protected area modifies its sound absorption and the velocity of sound waves traveling through it. Under normal conditions a uniform temperature change will not have an appreciable effect on the operation of the device. In

---

[87]"Automate Plant Protection," Factory, CXIX (December, 1961), 60.

[88]Bagno, op. cit., p. 51.

areas where temperature changes are large and abrupt this characteristic might prove to be a source of trouble.[89]

It is necessary that a sound wave system be used in a confined area. This normally does not create a problem since it can be accomplished by surrounding the protected area with practically any type solid material. Gypsum wallboard, plywood, or similar materials provide a satisfactory enclosure and reflective surface for the sound waves. Since sound waves are easily deflected by such materials, it prevents alarms caused by movement outside the protected area.[90]

Due to the low density of the hot air in a flame, it tends to reflect sound waves as a solid object. The rapid movement of the flickering flame and the cone of hot air above it has an effect similar to a moving intruder and will cause an alarm. The size of the flame that can be detected is dependent on the sensitivity setting of the control unit. At any given setting it will detect a flame about one-fourth the size of the minimum detectable intruder.[91] There have been cases in which a sound wave alarm device detected a fire sooner than standard fire detection instruments in the area. This is generally considered to provide additional protection and should not be used to supplant standard fire detection equipment since the

---

[89] Ibid.

[90] Walter Kidde and Company, op. cit., p. 11.

[91] Bagno, op. cit., p. 49.

intrusion detector is normally in operation only during non-working hours.[92]

Sound wave detection devices provide almost complete protection against "stay behind" intruders. They have a high salvage value and are easily removed and re-installed in a new area.

Sound wave detectors are susceptible to nuisance alarms caused by vibrations and loud outside noises. If a penetration into a protected area is made behind a large object located near the wall it may not cause an alarm. It is also possible that slow moving intruders (less than four steps in four seconds) may not be detected.[93]

Signal Wires

All proprietary and central station alarm systems in general use today employ signal wires to connect detector and sensing system control units with the monitoring equipment located in the guard room or central station.[94] The purpose of these lines is to transmit a signal which indicates that an intrusion has been made or is being attempted into a protected area. In addition to transmitting this

---

[92]Walter Kidde and Company, op. cit., p. 5.

[93]Mosler Research Products, op. cit., pp. 9-10.

[94]Minneapolis-Honeywell Company, Security and Equipment Surveillance Systems (Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated), p. 17.

signal the lines carry a specific amount of electrical current (normally five to twenty milliampres, direct current). Minor changes in this current cause an alarm signal at the guard room or central station.[95] This is referred to as line supervision and the instruments which perform this function are part of the monitoring equipment and will be described in the section devoted to that equipment.

In many cases the signal wires are leased from the telephone company but in proprietary systems they are more often owned and maintained by the protected firm.[96]

A direct wire or circuit alarm connection may be used with the signal wires. The direct wire connection provides a separate line between the protected area and the monitoring equipment. The circuit connection may link several widely dispersed areas on the same circuit. This is accomplished by using a coding mechanism in the protected area which transmits a different coded impulse for each area, sensing system, or detector. This impulse activates the proper alarm in the guard room or central station and identifies the location of the alarm condition.[97] Some manufacturers claim that as many as fifty areas or sensing

---

[95]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961), p. 23.

[96]Minneapolis-Honeywell Company, loc. cit.

[97]American District Telegraph Company, Electric Protection Services, Book II (New York: American District Telegraph Company, 1960), p. E1-2-3.

systems can be served by a single pair of wires through use of this circuit alarm connection.[98] Use of this system involves an inherent risk since malicious or accidental interruption of these lines might affect several areas simultaneously. Such a system cannot qualify for the best grade of Underwriters' Laboratories certification.[99]

Since a short circuit, broken wire, or other failure of the signal wires may render segments or the entire system inoperative it is necessary that they be properly protected and given emphasis equal to other components of the alarm system. The security provided by the system is no better than this important link.[100] In addition to the electrical line supervision, the lines must be given as much physical protection from accidental damage as possible. A proprietary system in which wires are located within property limits of the protected firm offer some protection and eliminate many of the signal wire security problems inherent in a central station system which uses public telephone wires. Signal wire systems should meet or exceed Underwriters' Laboratories alarm installation standards and specifications and should be regularly inspected. Additional

---

[98]Westinghouse Electric Corporation, Teltronic Systems, Bulletin 500-001 (Jersey City, New Jersey: Westinghouse Electric Corporation, undated), p. 3.

[99]American District Telegraph Company, loc. cit.

[100]Minneapolis-Honeywell Company, loc. cit.

specifications listed by the Army Ordnance Corps may also provide specific guidance for industrial installations.[101]

Monitoring Equipment

The basic functions of monitoring equipment are: to receive alarms and give an alarm signal, provide line supervision, and supply electrical energy. The equipment is manufactured by a variety of firms and selection of the proper type should be conditioned by individual plant needs.

Receiving Alarms. The primary purpose of monitoring equipment is to receive alarm signals from detector and sensing system control units and notify guards that an alarm condition exists. The method of accomplishing this varies with individual models but generally it gives an audible and visible signal by means of a buzzer or bell, and a small signal light. The audible signal eliminates the possibility that a signal light may come on and not be observed.[102]

All acceptable monitoring equipment must also cause a visible and audible signal to indicate a condition change or other trouble with the system, such as tampering with any part of the system, failure of parts of the system to function properly, and failure of the power supply. It is also important that such equipment be designed to permit frequent testing. The importance of this feature is

---

[101] Department of Army, Intrusion Detection Systems, ORDM 10-2, op. cit., p. 23-4.

[102] Ibid., p. 25.

illustrated by the fact that a recent inspection at a highly classified national security facility revealed that six out of twelve areas that were tested failed to give an alarm for power failures.[103]

Line Supervision. Monitoring equipment also contains the instruments and circuitry which provides electrical line supervision. Since signal wires are exposed to tampering over long distances it is not feasible to provide complete physical protection against such acts. It is thus necessary to rely on electrical supervision to provide line security. The instruments used for this purpose must be sensitive enough to detect attempts at compromise and be capable of sounding an alarm. Some of the methods used to defeat alarm systems are: (1) Substituting a resistance load equal to that of the devices in the circuit. (2) Applying current across the lines which is roughly equivalent to that normally present, which holds the relays in a closed position so a warning will not be given if a detector initiates an alarm.[104] If the wires can be compromised, the protected area may be entered without causing an alarm. Under normal circumstances a simple closed circuit may provide some protection against accidental conditions, but

---

[103]United States Army Supply and Maintenance Command, letter from Chief, Security Division, dated January 10, 1963.

[104]Department of Army, Intrusion Detection Devices, TB PMG 26 (Washington: Government Printing Office, 1959), p. 8.

offers little protection against a trained enemy agent or thief. Some commercial installations may be adequately protected by using overload and underload relays which will detect a forty per cent current change, above or below normal which may vary from ten to thirty milliampres. Such a tolerance, however, is sufficient to permit a skilled intruder to defeat the system.[105]

In order to provide adequate line supervision for high priority targets for espionage and sabotage the lines must be protected by highly sensitive line supervision circuits. One manufacturer uses an ultra-sensitive galvanometer relay for this purpose. This instrument will detect changes as small as twenty-five microampres.[106] Sensitivity equivalent to this is considered necessary by one government agency in order to provide effective line supervision.[107] This manufacturer states that the instrument provides sufficient sensitivity to detect the presence of moist finger tips on bared signal wires.[108] It may be necessary to reduce this sensitivity to compensate for normal current fluctuations produced by moisture or similar causes. Specifications prescribed by the Army Ordnance Corps require

---

[105]Mosler Research Products, Incorporated, op. cit., p. 15.

[106]Ibid.

[107]Department of Army, Intrusion Detection Devices, TB PMG 26, loc. cit.

[108]Mosler Research Products, Incorporated, loc. cit.

security systems under their control to have a line tolerance of one milliampre or less.[109] Since the weakest link in the security system is usually the signal wires they should be given special attention.

Current Supply. The monitoring equipment also supplies electrical power to operate the electrical components of the intrusion alarm system. Some detectors are operated from power available in the protected area while others operate on power supplied by monitoring equipment. As transistors come into more common use the number supplied by power from the monitoring equipment is expected to increase. Added protection is provided when electrical energy is supplied in this manner and this system should be used when feasible.[110]

Location and General Types. Monitoring equipment is normally located in a guard room or central station. In some large facilities, however, the system may be broken down into zones with segments of the equipment located at local control points in close proximity to the protected area. The purpose of using these local control points is to reduce the time required for guards to respond to alarms. It is desirable that local control points be connected with

---

[109]Department of Army, Intrusion Detection Systems, ORDM 10-2, op. cit., p. 24.

[110]Department of Army, Intrusion Detection Systems, ORDM 10-2, op. cit., p. 25.

the central guard room so personnel there are alerted that an alarm condition exists somewhere in that zone. This would prevent intruders from overcoming a guard and making an intrusion without the knowledge of personnel in the guard headquarters.[111]

Monitoring equipment is available in a variety of sizes and configurations. Selections for specific plants must be based on local needs. It may consist of a simple cabinet mounted on a wall or it may be an elaborate unit contained in an upright console or installed in a desk. Most monitoring equipment is of modular construction so the system can be easily reduced or expanded to meet changing security requirements. The monitoring equipment of many plants contains guard force communication equipment, television monitors, and equipment to monitor industrial processes and fire protection devices.

Persons monitoring the equipment must be able to identify immediately the location of alarms. This may be accomplished by arrangement of the equipment or through the use of identification cards placed on the face of alarm panels. One alarm manufacturer provides a graphic annunciator board which pinpoints the alarms on an actual representation of the floor plan or overlay of the protected area. The guard can thus immediately detect the exact location of any alarm. This system can only be used where

---

[111] Ibid., p. 29.

space is not limited.[112]

III. RECENT INTRUSION ALARM DEVELOPMENTS

Intrusion alarm manufacturers, just as other American industries, are continually conducting research in order to produce new and better equipment. Some firms are conducting research under government contract while others are interested primarily in improving service and sales in order to remain competitive with other manufacturers and protective companies. A good example of the latter group is the American District Telegraph Company. This firm has established a twenty acre field testing laboratory where tests under various weather conditions are conducted. The site facilities include a permanent building which serves as a control center, and contains a workshop and conference rooms. Prior to establishment of this facility selected customers were used to field test equipment. Now field tests of new equipment can be conducted under constant observation and necessary minor changes can be made immediately to correct defects.[113]

Research by companies under contract to the Federal Government is generally for the purpose of developing

---

[112]Minneapolis-Honeywell Company, W657A Security Monitor (Minneapolis, Minnesota: Minneapolis-Honeywell Company, 1954), p. 1.

[113]"Twenty Acres of Field Testing Facilities," ADT Transmitter, XXXII (December, 1960), 6-7.

equipment for protection of material or information of national security interest. For this reason, many of the developments are classified and can only be released on a "need to know" basis. They could not be included in this paper for that reason. It appears that firms with classified contracts would fall into this category and could avail themselves of this information through appropriate security officers.

There have been several recent developments in detection devices and methods of transmitting alarm signals from the protected area to the guard room or central station. In most cases the new equipment has been subjected to extensive laboratory tests and some field use but this has not been sufficient to permit complete evaluation.

Detection Devices. One of the latest detection devices is the radio frequency or "radar" detector. Several attempts to devise a detector of this type have failed but it appears future improvements may make this a useful device.[114]

The principle of operation is quite similar to the sound wave detector. In place of sound waves this detector emits high frequency radio waves in the range of the 350 megacycle band. If all the objects in the protected area

---

[114]Mosler Research Products, Incorporated, Electronic Anti-Intrusion Systems and Electronic Investigative Equipment (Danbury, Connecticut: Mosler Research Products, undated), p. 13-14.

remain stationary the reflected waves return to the receiver at the same frequency. If an object moves, the pattern is disturbed and an alarm is activated. Area coverage may be controlled to some extent by placement of antennae and adjustment of the transmitter. Since radio waves will penetrate ordinary walls it is usually necessary to reduce the power output to limit the protective field to the secured area.[115] In normal rectangular rooms this will generally leave "dead spots" which are unprotected. It is therefore desirable that the protected area be surrounded by reinforced concrete or similar material. It may also need to be shielded in order to provide complete protection and prevent false alarms caused by movement outside the area.[116]

The radar detector is not affected by air currents, noise, light, or sound. The equipment is compact and can be easily removed and re-installed in new areas to meet changing security requirements.[117]

There is still some question on the legality of operation of the device since the transmitter output exceeds Federal Communication Commission regulations. The stability of operation is also questionable and some models use

---

[115] Ibid.

[116] Department of Army, Intrusion Detection Systems, ORDM 10-2, op. cit., p. 19.

[117] Mosler Research Products, Incorporated, op. cit., p. 19.

electron tubes which require one hundred and ten volt alternating current.[118] Some models have been used at government facilities and one alarm manufacturer claims that they give foolproof and reliable service at these sensitive installations.[119]

One manufacturer is experimenting with a detector which employs double pane windows with pressurized gas between the panes. An alarm would be initiated by even a small crack in one of the panes. This detector could provide dependable protection without detracting from the appearance of the window.[120]

Another device consists of a printed circuit which can be used as a merchandise tag in a retail store. When the article with this special tag attached passes a radio transmitter and receiver, tuned for different frequencies, the printed circuit converts the transmitting frequency to the response frequency of the receiver and causes an alarm. A major alarm manufacturer considered use of this device but decided against it. The manufacturer indicated that they thought the device had been patented but a record

---

[118] Ibid.

[119] Singer-Bridgeport Company, SWAMI Motion Detector (Bridgeport, Connecticut: Singer-Bridgeport Company, undated), p. 3.

[120] "Twenty Acres of Field Testing Facilities," loc. cit.

of the patent could not be found.[121]

Another interesting possibility is the use of radioactive isotopes with a geiger counter as a detection device. Classified documents and/or material within an enclosed area could be given a slight radioactive "charge." Geiger counters located at the exits would sound an alarm if a person attempted to remove the documents or material from the area. One major manufacturer conducted some experimental work with such a device but discontinued work due to concern over possible radioactive hazard and the fact that regulations covering its use were too cumbersome. This manufacturer indicated that, to their knowledge, no one was using such a device and technique at that time.[122]

Alarm Transmission Equipment. New methods of transmitting alarm signals from the protected area to the guard room or central station are under development. Since signal wires are generally the most vulnerable component of the intrusion alarm system this could prove to be a very significant development.

One alarm manufacturer uses infrared beams for the purpose of transmitting signals but this technique is apparently still in the development stage and little descriptive

---

[121]American District Telegraph Company, Letter from Mr. G. G. N. Purcell, Public Relations Department, dated March 29, 1963.

[122]Ibid.

information was available.[123]

Another firm uses carrier circuits similar to those used by telephone companies to transmit signals via a number of high frequency channels. Coded alarm signals could thus be transmitted with comparable equipment. This system has been adopted on a limited scale and it is said to operate in a satisfactory manner in some areas. The next step planned is establishment of "satellite stations" which are connected by short wires with protected premises. The "satellite stations" would be designed to receive and automatically retransmit alarm signals from the protected area to a central station.[124]

IV. THE ROLE OF UNDERWRITERS' LABORATORIES

A study of intrusion detection equipment would not be complete without a discussion of the relationship between Underwriters' Laboratories and the intrusion alarm industry.

This organization is a non-profit corporation which was established in 1894 to operate laboratories for the examination and testing of devices, systems, and materials. It is sponsored by the National Board of Fire Underwriters and is operated for service rather than profit. The nature

---

[123]Minneapolis-Honeywell Company, Security and Equipment Surveillance Systems (Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated), p. 17.

[124]Maxwell H. A. Lindsay, "ADT Takes a Giant Step," The ADT Transmitter, XXIV (May-June, 1962), 7.

of the business, objects, and purposes to be transacted are stated in the certificate of corporation as follows:

> By scientific investigation, study, experiments, and tests, to determine the relation of various materials, devices, constructions, and methods to life, fire, and casualty hazards, and to ascertain, define, and publish standards, classifications, and specifications for materials, devices, constructions, and methods affecting such hazards, and other information tending to reduce and prevent loss of life and property from fire, crime and casualty.[125]

A manufacturer may voluntarily submit his product for testing and if it does, the expenses incident to the tests are chargeable to the manufacturer. The laboratories publish standards and lists of approved products and conduct follow-up inspections to insure that proper standards are maintained. The Burglar Protection Department of Underwriters' Laboratories is located at 2550 Dundee Road, Northbrook, Illinois.[126]

Shortly after World War I hundreds of companies entered the burglar alarm business. Many of the alarms were nothing more than simple open circuits similar to a doorbell circuit. The high burglary rate during this period caused merchants to turn to these simple alarms for protection. They were encouraged by insurance companies which offered inducements in the form of reduced premiums to firms that installed the equipment. Losses continued to be

---

[125]Underwriters' Laboratories, Testing for Safety (Chicago: Underwriters' Laboratories, 1959), p. 7.

[126]Ibid., pp. 6-26.

extremely high and many of the thefts occurred in premises that were "protected" by electrical alarm systems. The insurance companies soon reversed their position which had an immediate adverse effect on the alarm industry. Reputable alarm manufacturers agreed to form a joint committee with representatives of insurance companies, and the Underwriters' Laboratories to discuss basic protective alarm standards. From these meetings the requirements for Underwriters' Laboratories approval were developed. The laboratories began conducting tests of alarm equipment which was submitted for testing and issued certificates for items which were acceptable. Insurance companies used these ratings to determine insurance premiums so many "fly-by-night" alarm companies were forced out of business. Legitimate firms then went to work in earnest to develop better alarm systems.[127]

Since the inspection is not mandatory some firms may not submit their equipment for testing. Most of them, however, submit to the tests in order to use reduced insurance rates to increase sales.

It should also be noted that the standards established by Underwriters' Laboratories are minimum acceptable requirements for alarms for a specific application. Product design and performance may go far beyond this minimum

---

[127]Mosler Research Products, Incorporated, op. cit., p. 2.

standard. Some equipment may exceed the requirements of Underwriters' Laboratories and not be listed because the nature of the installation or class of equipment may not fall into one of the categories which have been established. The Underwriters' Laboratories standards are generally related to the protection of commerce and industry against ordinary theft. The requirements for security of industrial plants with classified government contracts and military areas may go far beyond those for mercantile alarm systems.[128]

It would be foolish, however, to ignore these standards which are based on extensive laboratory and field tests. A field service report is maintained by the laboratories which lists the number of attacks on certificated installations and analyzes system failures. This record is brought up to date each year and republished. In 1961 it reflected the performance of approved systems over a 14 year period.[129] This publication is for restricted distribution and the results of the record cannot be listed here but the results of approved systems are very impressive. One indication of the reliability of the approved equipment is the fact that insurance companies will reduce burglary insurance premiums as much as 70% when such equipment is installed.[130]

---

[128] Ibid., p. 3.

[129] Underwriters' Laboratories, 1961 Field Service Record (Chicago: Underwriters' Laboratories, 1962), pp. 8-9.

[130] Robert Gorman, "The War Between Burglars and Inventors," Popular Science, CLXXVI (April, 1960), 92.

It can be expected that trained enemy agents will be more skilled than an ordinary burglar and the success of this equipment in preventing sabotage and espionage might be less impressive. With this limitation in mind, this record might be related to protection against such acts.

CHAPTER IV

CLOSED CIRCUIT TELEVISION

Television is the transmission of a picture from one location to another through use of an electrical signal. This means that a series of images is picked up at one location and transmitted to another in such a way as to give apparently continuous reproduction of pictures. The basic difference in closed circuit television and well known commercial television broadcasting is the means used to transmit the signal between the two terminals. If the signal is radiated on an assigned channel, it is broadcasting. If it is viewed only at points where it is delivered by coaxial cable or microwave relay, it is a closed circuit system.[1] All known security applications employ the closed circuit system.

Some publications consider closed circuit television as another type of intrusion detection system. This position is supported by pointing out that the components of both are functionally similar. That is, both contain a sensing system, means of transmission, and equipment to

---

[1]Morris A. Mayers and Rodney D. Chipp, Closed Circuit Television System Planning (New York: John F. Rider, Publisher, 1957), p. 107.

monitor signals received from the sensing system.[2] This may be true, but it was felt that there were sufficient differences in the characteristics and uses of the two systems to justify a separate chapter for each. It is likely that many security systems will employ both in a mutually supporting role.

In order to understand possible security applications of closed circuit television it is necessary to explain the development of closed circuit television, the components of the system, and general security applications of the system.

I. DEVELOPMENT OF CLOSED CIRCUIT TELEVISION

The history of closed circuit television is much shorter and less colorful than that of intrusion detection systems. It evolved from commercial television and has drawn heavily on technical knowledge gained as a result of research conducted by the commercial television broadcasting industry. It is fortunate that this was possible because the research necessary to develop closed circuit television would not have been economically feasible without this "shared" information.

Prior to World War II an extensive program of

---

[2]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961), p. 22.

research and development was carried out which resulted in the establishment of standards for good black and white television practice.[3]

During the war television was employed for the first time as an observational aid. Its principal use during this period was for aerial reconnaissance by relaying images from airplanes and guided missiles to stations on the ground. After the war the commercial television broadcasting industry expanded rapidly and national networks were established in several countries.[4]

One of the first commercial "service" applications of closed circuit television took place in 1946 when the officers of two large firms signed a contract while separated by two hundred and fifty miles via two-way closed circuit television. In the ten year period that followed, closed circuit television in industry grew from one fixed camera trained on a water gauge to installations with one hundred cameras with a switching system which permitted selection of any one subject for viewing. Cameras used by industry have evolved from heavy, cumbersome pieces of equipment, which required a six-man crew, to tiny self-contained units slightly larger than a package of king-sized

---

[3]Radio Corporation of America Service Company, Closed Circuit Television Systems (Camden, New Jersey: Radio Corporation of America Service Company, 1958), p. 1.

[4]H. A. McGee, Industrial Television (London: Wyman and Sons, Limited, 1957), p. 1.

cigarettes. The original stationary camera was replaced by cameras equipped for vertical and horizontal movement which contain equipment for remote control of movement, and lens and iris settings to compensate for changing conditions.[5]

Initially the television industry found itself in the position of meeting specifications for closed circuit television systems requested by industry as industry discovered new applications for the system. These uses were usually to solve problems involving conditions which were dangerous to human life. As industry gained confidence in the system it began to find other applications. As television engineers observed the various applications they provided a stimulus to further development by serving as a channel of information between various industries.[6] Closed circuit television is now in extensive use in industry, commerce, medicine, the armed forces, and education.

Security applications have not increased as rapidly as other fields and security personnel appear to have adopted a "wait and see" attitude. This is possibly due to lack of information, resulting in lack of confidence in the equipment for use as an aid to security. The apparent

---

[5]M. A. Mayers and R. D. Chipp, Closed Circuit Television System Planning (New York: John F. Rider, Publisher, 1957), p. vi-vii, foreword.

[6]E. C. Carroll, "Closed Circuit Television for Industrial Applications," Iron and Steel Engineer, XXXVII (July, 1960), p. 78.

feeling is that security is too important to gamble with. For these reasons plant security directors and cognizant security officers who inspect plants with classified government contracts are hesitant to approve use of the equipment without further field testing and evaluation. These problems should be overcome as additional data concerning reliability in field use become available through professional magazines and government publications. Since cost of the equipment is apparently an important factor, subsequent price reductions will also stimulate use. Some authorities feel that it is not unreasonable to expect that small, completely transistorized cameras that will feed standard receivers will soon be on the market at prices low enough for domestic use. If this occurs, then the cost of the equipment will become an insignificant factor in use of the equipment in industrial plant security.[7] At the present time most security applications are limited to prevention of thefts in retail establishments rather than prevention of sabotage, espionage, and other forms of subversion in industrial facilities.

II. COMPONENTS OF A CLOSED CIRCUIT SYSTEM

Although detailed knowledge is not required, security personnel planning a closed circuit television system

---

[7]Mayers, op. cit., p. 186.

must have a general knowledge of the equipment and its capabilities. A layman's knowledge of the component parts and their function is sufficient for basic planning, but before the plan is complete, technical assistance must be secured. In industrial plants management will require that specifications be accurately stated so consultation with a technician is mandatory to prepare the technical portion of contract specifications. The basic components of all closed circuit systems, from the simplest to the most complex, consist of a camera, interconnection system, and monitor. These components will be discussed in detail in this section.

Camera. The camera in a closed circuit television system is comparable to the sensing component of intrusion detection systems. Several manufacturers make cameras which are suitable for security applications. In general they are much smaller than conventional studio cameras; as indicated earlier some of them fit neatly into one hand and are only slightly larger than a king-sized cigarette package. As additional advancements in transistorized circuitry and miniaturization of parts are made this will no doubt permit further size reductions. Most industrial television cameras will operate satisfactorily on a conventional one hundred and ten volt alternating current power source. Some models operate on less than fifteen watts which is about one-seventh the power used by a regular home light bulb.

If cameras are to remain stationary a very simple mount is adequate and it may be attached to practically any surface. They are commonly mounted on walls and ceilings, or special posts when other mounts are not available. If it is desirable to move a camera horizontally or vertically a "pan and tilt" mount may be used. Such remotely controlled mounts permit as much as three hundred and fifty-nine degrees horizontal and forty-five degrees vertical movement.[8]

Mirrors have also been used in some special applications to provide additional area coverage. As an example, a movable mirror has been used in lieu of the pan and tilt mount.[9]

If cameras are used outdoors a weatherproof housing should also be provided to provide protection from cold, moisture, and dust. A deceptive housing can also be used to conceal the camera and permit unobserved operation. If a weatherproof or other housing is required, it should be thoroughly checked to insure that it can accommodate other accessories, such as special lenses, that might be needed for a particular operation.[10]

One of the more important parts of the camera is

---

[8]Walter L. Rochette, "Closed Circuit Television; New View for Business," Personnel Journal, XXXIX (March, 1961), 409-412.

[9]Mayers, op. cit., p. 146.

[10]Ibid., p. 212.

the lens which might be considered the "eye" of the system. In security applications the camera is generally unattended and in a stationary position except for "pan and tilt" movements. It is, therefore, impractical to consider moving the camera closer or farther away from the subject to attain either more detail or picture coverage. With some systems, containing an intercommunication system, a person can be asked to move closer to the camera but this is not always practical or desirable. This problem may be eliminated, however, by proper selection of lenses which will allow viewing of subjects in various degrees of detail from a fixed camera position. A wide angle lens (short focal length) tends to broaden the field of view and gives an appearance that the subject has been moved away from the camera. On the other hand, a telephoto lens (longer focal length) will give a narrower field of vision and gives the appearance that the subject has been moved closer to the camera. A single lens can be mounted in the camera but a great deal of flexibility can be achieved by mounting lenses of short, standard, and long focal length in a turret. Remote control of the turret allows the operator at a remote location to view a wide area with little detail or a narrow area with increased detail. The operator can thus monitor a large area until suspicious activities are observed, then "bring it in close" for a better view. One disadvantage in the use of the turret lens arrangement is that a brief

loss of contact is experienced during the rotation of the turret to change lenses. Through use of a zoomar lens it is possible to do the work of several lenses and eliminate the problem of loss of contact experienced with multiple lenses. The zoomar lens is usually more expensive and normally cannot achieve a maximum iris opening equivalent to standard lenses.[11]

Generally speaking, if a person can see a subject easily with normal vision, modern industrial television can also see it. The primary limiting factor is the amount of available light on the subject to be viewed. Television requires about as much light as a person does for good, clear visibility. The light found in offices, work areas, and daylight outdoors is sufficient to produce clear television images. Outdoor areas at night, warehouses, and stockrooms normally will not produce clear pictures unless artificial illumination is provided. Persons familiar with photography will have little difficulty determining light requirements for television. A standard light meter is an excellent means of measuring the light level. In most cases a reading of five to twenty-five foot candles will be sufficient for a satisfactory picture. There may be some "snow" in the picture, but it should be equivalent to that of a good home receiver. Up to a certain point,

---

[11] Mayers and Chipp, op. cit., pp. 141-146, 216.

as the level of light increases, the quality of the pictures improves; however, very bright light must be compensated for by reducing the amount of light admitted. Conversely, as the amount of light decreases, the lens iris must be opened to admit more light. Obviously, if the amount of illumination varies significantly, it will be necessary to provide some means of adjusting the lens iris to take full advantage of available light. This may be accomplished automatically by a built-in light meter type device, manually at the camera, or from the guard room through use of a remote control device. It is desirable that lenses for security applications have a maximum iris opening of f1.5 to f2.0 to be most effective. It is also desirable to use a lens which can be focused from a remote location to give additional clarity to the picture.[12]

Interconnection System. The interconnection system of a closed circuit television system is comparable to the signal wire component of intrusion detection systems. It connects the television camera with the monitor and thus bridges the gap of space between the two. By extending vision it permits the guard to watch many widely separated areas from one place. If the distance covered is less than two thousand feet, it may consist of a simple coaxial cable. If it is desired to increase this distance amplifiers may

---

[12] Ibid.

be used along the cable. Additional amplifiers may extend this to several miles if necessary. For greater distances a microwave relay system may be employed.

In addition to these two forms of transmission, there has been some experimentation with the use of light beams to carry this signal. This has been done successfully in laboratories but its range is still too limited to be of value.[13]

Controls for lens focus, iris setting, "pan and tilt" movements, and switching cameras are a part of the interconnection system and can be operated from a single control unit located in the guard room. The procedure for such adjustment is similar to adjustment of standard home receivers and should require little additional training.[14] One manufacturer found that it was desirable to limit the number of adjustments possible to a minimum to reduce unnecessary tampering.[15] This component is important because much of the versatility and effectiveness of the entire system will depend on its proper functioning.

Monitor. The monitor completes the closed circuit system. It is comparable to the monitoring equipment in an intrusion detection system with one important difference.

---

[13]Mayers, op. cit., 110.

[14]Radio Corporation of America Service Company, op. cit., pp. 171-172.

[15]Rochette, op. cit., p. 411.

Current closed circuit television monitors give only a visible signal to indicate changes in the viewed area. Unless combined with other systems there is no audible signal to bring the attention of the guard to the monitor. For this reason closed circuit television is often employed with intrusion detection equipment or other signalling systems to draw attention to the monitor or cause the guard to switch to the proper camera.[16]

A monitor for security applications should meet the requirements of high contrast, extra brightness, good resolution, long-time picture stability, and long life operation. The monitor needs high contrast since the signal must often travel long distances from the camera and may originate in poor light. Extra brightness may be required due to the presence of bright light in the viewing area. Better resolution enables the viewer to see more detail. Picture stability is necessary to avoid frequent monitor adjustment. Finally, long life components are desirable to minimize time lost due to repair. Although all other parts of the system may function perfectly, a poor monitor will produce a poor picture.[17]

A standard home receiver may be used but will generally not provide performance equivalent to industrial

---

[16]Department of Army, op. cit., p. 22.

[17]Mayers, op. cit., pp. 122-128.

monitors. Such receivers are often used for the sake of convenience or economy but must be modified to handle closed circuit television signals.[18]

III. SECURITY APPLICATIONS

The uses of closed circuit television in industrial plant security activities are limited only by the ingenuity and imagination of the security planner and the capabilities of the equipment. With a general understanding of the available equipment it is possible through application of deductive reasoning to consider possible uses in a plant security system.

In addition to an understanding of the equipment, it is also helpful to study applications which have been used in order to profit from the experience of others.

Closed circuit television has been used for employee identification, vehicular control at gates and doors, and surveillance of interior and exterior areas. The purposes of area surveillance may include prevention of unauthorized entry, detection of pilferage, or to insure compliance with company rules and policies. Since the primary emphasis of study is industrial plant security, applications of closed circuit television equipment to retail security and installations designed for the primary purpose of theft

---

[18] Ibid., 113.

prevention or to insure compliance with company rules were not considered. It is possible that the uses discussed may also serve these purposes but it would only be of incidental or secondary importance. The use of closed circuit television to "spy" on employees raises many collateral issues and has been avoided in this study. This is not to say, of course, that flagrant violations would be ignored simply because it was observed through use of closed circuit television equipment.

Identification. Personnel identification is one of the principal uses of closed circuit television in plant security activities. Employees are normally identified before entering the general area of a facility or certain controlled areas within. Although the degree of security may dictate a very detailed examination, the procedure is generally the same. The guard compares the employee's face with his picture on a badge at controlled entrances. It is possible to connect these points to one office by closed circuit television so a single guard can control access at several entrances. In addition to identification, the camera should be installed to give the guard a view of the general area surrounding the entrance. When the picture on the badge appears on the monitor it should be about the same size as the image of the employee's face. Two-way communication between the guard and the employee desiring entrance should be provided to permit an exchange of information and instructions. A standard intercommunication

system or telephone is sufficient for this purpose. Once identification is made the guard should be able to permit entrance and at the same time deny access to others. Electrically controlled gates or doors operated by a guard can serve this purpose. Employee identification by the use of television is generally most effective when the number of employees is small. This same limitation applies, however, in any system involving comparisons of badges and individuals.

One firm has successfully used this system by installing two cameras at an electrically controlled gate. One camera overlooks the gate and gives a clear view of the person desiring access. The second camera is mounted at about waist height. Employees place their badge in front of the second camera and press a button which sounds a buzzer at the guard office. At a glance, a comparison of the two images is made and when the guard is satisfied with the identification he presses a button which unlocks the gate so the employee can enter. As he enters one of the cameras provides a full view of the gate and precludes entrance by other persons. If questions arise during this identification procedure, an intercommunication system permits conversation between the two points.[18]

Another method of employee identification is provided

---

[18]"TV Goes on Guard for Esso," Oil and Gas Journal, LV (March 18, 1957), 98.

through use of a special dual lens. With this lens the camera splits the image into two parts. One part of the lens shows an image of the employee and the other part shows the picture on his badge. In order to accomplish this the individual approaches the camera and places his badge in a holder; he then steps back to a mark on the floor. The guard views both images which appear about the same size on a single monitor. After identification an electrically controlled gate permits entrance.[19]

Another application uses one camera in combination with a special field lens. An employee desiring entrance stands at a designated spot about twelve inches in front of the camera. He then places his pictured badge in a guide and moves the guide to a position about six inches to one side of his face. A field lens in the guide apparatus magnifies the picture to about one-fourth or one-half the size of the employee's face. A single monitor in the guard office portrays both images. Although the reproduction of the badge is smaller than with other systems it is pointed out that a guard physically present at the entrance only sees a picture about one-tenth the actual size of the face when making comparisons.[20] When television is used for

---

[19]Mayers, op. cit., p. 146.

[20]Allen B. DuMont Laboratories, "Selling the Security Market" (Clifton, New Jersey: Allen DuMont Laboratories, undated), pages unnumbered (mimeographed).

control of entrances and exits from a building it is generally better to locate the camera inside the building for greater protection from tampering and protection from the elements.

Vehicular Control. Vehicle control offers another effective use of closed circuit television when there is a small volume of traffic and detailed inspection is not required. Electrically controlled gates and an intercommunication system are also generally included as a part of this system. Nights, weekends, and holidays are particularly suitable, and many entrances used during normal hours may be controlled in this manner. A stopping point for the vehicles should be selected which will place the vehicles in the desired location for the camera. It should also permit the gates to swing open freely if they are of this type construction. Instructions for gaining entrance should be prominently posted at the gate. Some installations use a photoelectric or other signaling device to alert the guard to the approach of a vehicle.

Closed circuit television is used at one facility to provide continuous control of entrances into a garage building. The building has three doors of the overhead type which are electrically operated, with a television camera mounted over each door. The system contains a two-way communication system which is also connected to each door. If a person desires admittance he is required to dismount from his vehicle and press a button which signals

the person at the monitor. After identification is made the guard opens the door and the person can drive his vehicle inside. Since the cameras are outdoors they are enclosed in weatherproof housings which contain a "windshield wiper," fan, and heater. The system also includes floodlights for periods of poor visibility.[21]

Area Surveillance. Television can be used for effective surveillance of both interior and exterior areas. Where it is desirable to maintain a surveillance of offices, document repositories, or similar areas cameras may be permanently installed for this purpose. With a remotely controlled, zoomar lens, and "pan and tilt" mount complete coverage of an area is possible and even covert attempts at sabotage or espionage can be detected. If light levels vary significantly an automatic or remotely controlled iris may also be necessary. Such a system would also be useful in keeping sensitive areas under observation during lunch periods, at quitting time, and at night during down periods. The specific location of the camera would be dictated by the layout of the room and its occupants. The best location is generally at the junction of the ceiling and wall, or it may be positioned on the ceiling at the center of the area. It may be desirable to disguise the opening for the camera by the presence of an air vent, lighting fixtures,

---

[21]"TV Camera for Garage Doors Provides Low Cost Plant Security," Gas Age, CXIX (November 23, 1961), 10-11.

or other common object.[22]

One firm with a classified government contract uses television for control of four closed areas. All entrances to the areas are monitored by a guard in the guard room. Open microphones are placed in the protected rooms so the guard can hear a noise if someone enters. By means of a public address system he can challenge anyone that enters or dispatch guards through use of a coded signal on a public address system. Unscheduled tests of the system have resulted in immediate observation and guard response within two minutes.[23] Recently this system was modified to include stationary mirrors placed directly in front of the cameras. The mirrors are placed at an angle which enables viewing of two doors in different parts of each room. One-half of each monitor screen at the guard room shows a door directly in front of the camera and the other half shows another door in the mirror reflection.[24]

Small, scattered security areas have always created special problems for industrial security personnel. In many cases the purpose of observation is to detect the

---

[22]Radio Corporation of America Service Company, op. cit., p. 183.

[23]Lee F. Malone, "Control of Closed Areas by Closed Circuit Television," Industrial Security, II (April, 1958), 8.

[24]Lee F. Malone, "Modern Electronics Assisted by the Age Old Mirror," Industrial Security, VII (January, 1963), 12.

presence of intruders during non-operational periods. Storage areas, electrical sub-stations, and equipment locations fall into this category. If a closed circuit television system for surveillance of such an area is only intended for night use, artificial illumination will be necessary. If designed for both night and day use an automatic or remote controlled lens iris will also be necessary. The placement of the camera in such a system would be dictated by the layout, the area to be observed, and information desired. If detection is the purpose, a fixed camera with a standard lens may be suitable. If the layout is not compatible with a simple installation, identification of intruders is desired, or if it is necessary to determine exactly what intruders are doing, a more complex system with zoomar lens, and "pan and tilt" mount, may be appropriate. With proper placement and use of an oscillating sweep, one camera can be used to monitor a large area. In such an installation the normal protective lighting on the fence line may provide adequate illumination for operation.[25] Such a system has been used effectively for detection of fires in an industrial facility during periods of darkness. The camera uses an oscillating sweep at a given inclination and is mounted on a rooftop to provide maximum visibility. If a fire is observed the guard can stop the sweep and use a

---

[25]Radio Corporation of America Service Company, loc. cit.

zoomar lens to provide a more detailed view. Marker lights are necessary in this system so a guard can orient himself as to direction.[26]

Consideration has been given to the use of closed circuit television for perimeter or fence-line surveillance and it is understood that the Atomic Energy Commission employs such a system at some of its installations. Additional information on such use was not available, however, due to the classified nature of its activities.

It appears that the greatest problem in use of television for area surveillance is the possibility of guard fatigue and subsequent lack of alertness. The guard can easily grow tired of watching a static picture on a television monitor and fail to detect intrusion or other unauthorized activity.

Discussion. One government agency considers a closed circuit television system the closest approximation to having a guard physically present in an area.[27] Another agency with numerous classified installations under its supervision declines to make recommendations on use of such a system due to limiting factors such as weather, lighting, and cost of the equipment. This agency further indicates that

---

[26]"Newest Roof Fire Watchman for Remote Control TV," Factory, CXIV (March, 1956), 91.

[27]U.S. Army Intelligence School, Electrical Protective Systems (Fort Holabird, Maryland: U.S. Army Intelligence School, 1962), p. 10 (mimeographed).

additional study and evaluation is required prior to full acceptance.[28] Some of the security directors that are actually using the equipment are convinced that it is definitely an effective aid to security if it is properly planned and used.[29] As with any other security aid, faulty planning may lead to disappointing results.

---

[28]Department of Army, Intrusion Detection Systems, ORDM 10-2 (Washington: Government Printing Office, 1961), p. 23.

[29]Malone, "Modern Electronics Assisted by the Age Old Mirror," op. cit., p. 12.

CHAPTER V

LIMITATIONS OF THE STUDY

The number of facilities studied was limited by several factors. It was necessary to restrict the geographical coverage in order to keep expenses and time requirements at a reasonable level. Within the geographical area selected (Wayne County, Michigan) the number of industrial facilities which employ the equipment and would grant an interview was also restrictive.

In interviewing security directors of large corporations it was found that they were reluctant to reveal security techniques or procedures which could result in monetary savings. They were concerned about protecting security "know-how" as well as cost-cutting production techniques. If a security technique is developed or discovered by one company that can result in monetary savings, the firm will attempt to keep this information from competitors. One security director spoke of keeping as much "lead time" as possible (in security practices) between his firm and its competitors. As a result, information on recent and more efficient security systems was not available.

One firm would not allow the researcher to visit any of its facilities and would not identify the plant which was used as an example to show the effect of use of the

equipment on security guard personnel requirements.

Persons interviewed did not want an "outsider" to take a close look at their security system. It was thus impossible to make an independent determination of the relative level of security provided through use of the equipment compared with use of security guards.

Another problem in this area is the fact that there is no scale or standard unit of measure to determine or describe a given level of security so valid comparisons can be made. One method which might be used to establish relative levels of security provided by the equipment versus manpower is to conduct unscheduled intrusion attempts while using only guards and make similar attempts using the equipment. This was not practical in this study since it was obvious that the security directors interviewed would not agree to such "tampering" with their security systems. The validity of general application of such tests is also limited. The degree of security provided is dependent on the alertness and effectiveness of the guard on duty, so when this important variable is changed such test results would not be valid.

Three of the firms interviewed were under some form of Federal Government security supervision. In these cases the inspectors generally agreed that security provided by the equipment was substantially equivalent to security provided by a given number of guards as indicated by the

security director. An attempt was made to determine the criteria applied by these inspectors to evaluate relative levels of security. Once it is established that the equipment meets or exceeds the standards established by Underwriters' Laboratories and is installed in accordance with their specifications, a "common sense" evaluation is made to determine if the equipment can be used to supplant guards. This opinion by the inspector is of limited value in comparing security provided by intrusion detection equipment and closed circuit television as opposed to security provided by a given number of guards.

Due to this lack of a common standard and an objective evaluation it was necessary to rely primarily on the opinions of security directors concerning levels of security provided. Their bias on this matter has been pointed out previously. In some cases they have been responsible for purchase or use of the equipment and will feel obligated to defend its use. On the other hand, some security directors feel that their status in the company is determined by the number of men under their supervision so they will be reluctant to admit that the equipment will supplant manpower resulting in a drop in their status.

There are several factors which must be considered in attempting to apply the information found in this study to other sections of the United States. The wages paid to security guards may vary widely. Some security directors

in the Detroit area are reluctant to use closed circuit television or intrusion detection equipment to replace manpower due to the high level of unemployment in that city.

The service rendered by local protection companies in supervising and maintaining leased equipment may also have an impact on the effectiveness of the equipment. In Detroit this service is apparently very good since some security directors have completely eliminated on-site guards and have installed equipment which is monitored and responded to by protection company guards. The quality of this service may vary widely in different sections of the United States.

These are some of the more important factors that must be considered before applying the findings of this study to other geographical areas.

CHAPTER VI

ANALYSIS

A sample of the schedule used to conduct interviews is contained in Appendix A. A recapitulation of responses received is contained in Appendix B.

Of the seven facilities studied two used closed circuit television in combination with an intrusion detection system to call attention of the guard to the proper monitor when an intrusion attempt is made. The other five facilities studied used electromechanical intrusion devices. All of the firms used the equipment to protect buildings or rooms within a building.

Four of the protected facilities considered were used for production; two for storage; and one was used for research and production.

In all but two cases the equipment was leased rather than purchased. Apparently good service is provided by protection companies for leased equipment in the Detroit area since persons using it were satisfied with this arrangement. The two facilities interviewed which used purchased equipment employed closed circuit television as the major component of the system. Closed circuit television is not presently available from protection companies on a lease basis.

All security directors interviewed felt that use of closed circuit television and/or intrusion detection equipment increased the effectiveness of the guard force. In five cases it actually eliminated the need for on-site guards. In these five facilities alarms are received by a central station operated by protection companies. Protection company personnel receive alarms and their guards and/or local police are dispatched to investigate.

As a result of the survey it was found that the total annual cost of one security guard in the geographical area studied, including wages, fringe benefits, equipment, etc., was generally in the $7,000 to $8,000 range with only one exception. The responses by facility to the question concerning the estimated annual cost of one security guard is shown below:

FACILITY	ESTIMATED TOTAL ANNUAL COST FOR ONE GUARD
A	$7,000.00
B	$8,000.00 if hired by the firm; about $5,000.00 if a contract guard service is used.
C	$8,000.00 if hired by the firm; about $5,000.00 if a contract guard service is used.
D	$7,000.00
E	$8,000.00
F	$3,000.00. This firm has no experience with guards but gave this as an estimate.
G	$7,000.00

Security directors of two facilities indicated that the cost of guards obtained from contract guard companies was from $2,000 to $3,000 per year less than guards hired by the protected company. According to these directors these contract guards performed satisfactorily.

In four of the facilities studied the equipment was installed after the guard force became operational. In the other three it was installed before the guard force became operational.

It was difficult to determine if an actual reduction of total strength of the guard force was possible as a direct result of use of the equipment. Three facilities which used leased intrusion detection, automatic fire protection, and industrial monitoring equipment as a "package deal" felt that the savings resulting from use of any one of these could not be considered separately. As an example, if only intrusion detection equipment was installed it would still be necessary to have a guard on the premises to provide fire protection and/or monitor industrial processes. For this reason the leasing fees used for these facilities in this study include the total fee for automatic fire protection and/or industrial monitoring equipment, as well as the cost for intrusion detection equipment.

In two of the facilities which installed closed circuit television and intrusion detection equipment after the guard force was operational, an actual reduction in the

size of the guard force was not made. The equipment was installed at a time when security had to be greatly increased in order to qualify for classified defense contracts. In the opinion of the security directors and government inspectors involved, installation of the equipment prevented an increase in the guard force to provide this additional security rather than making a reduction possible.

It is felt that the best indication of the monetary savings resulting from use of the equipment was obtained when security directors were asked to estimate the number of guards that would have to be added to the guard force to maintain the same level of security if the facility discontinued use of intrusion detection and/or closed circuit television equipment. In response to this question security directors indicated that the following additional guards would be required:

Facility Identification	A	B	C	D	E	F	G
Estimated number of additional men	9	3	3	3	0	2	2

To determine the theoretical monetary savings under these conditions the number of men which would have to be added was multiplied by the annual cost of one guard and compared with the total cost of using the equipment. In the case of purchased equipment this total cost included initial purchase price, installation, maintenance, and annual depreciation (initial purchase price divided by the life expectancy of the equipment). In the case of leased

equipment this total cost included the installation cost and the annual leasing fee, which includes maintenance.

Through use of this theoretical comparison it was found that six of the seven firms studied would experience a monetary saving during the first one year period. After the first one year period the amount of saving rises since funds for initial purchase and/or installation would be expended during the first year. As additional years are added it spreads these initial costs over a longer period. The security director of one facility indicated that additional guards would not be required if he discontinued use of the intrusion detection equipment. Most of the effort of this guard force is devoted to fire protection and industrial monitoring and based on past experience illegal entry had not been a serious problem. This director thought intrusion detection equipment increased the effectiveness of his guard force but felt that the same number of guards would be required to perform fire protection and industrial monitoring duties if intrusion detection equipment was not used.

The results of this theoretical comparison projected over one, five and ten year periods is shown below:

FACILITY	SAVINGS OVER ONE YEAR PERIOD	SAVINGS OVER FIVE YEAR PERIOD	SAVINGS OVER TEN YEAR PERIOD
A	$49,900.00	$295,500.00	$602,500.00
B	7,500.00	97,500.00	210,000.00
C	7,500.00	97,500.00	210,000.00
D	14,550.00	96,750.00	199,500.00
E	0	0	0
F	4,900.00	24,500.00	49,000.00
G	5,500.00	45,500.00	85,500.00

CHAPTER VII

CONCLUSIONS AND PROBLEM AREAS WHICH NEED ADDITIONAL STUDY

As the researcher conducted interviews and attempted to formulate conclusions based on these interviews it seemed that few properly supported conclusions could be drawn. Due to the limited number of facilities studied (7) and the restricted geographical coverage (Wayne County, Michigan), it is necessary that caution be used in making generalizations concerning the effect of use of the equipment on guard force personnel requirements and resultant monetary savings. On the other hand, many questions were raised which need more research. In short, the study yielded more questions than answers. Perhaps this should be expected in a professional field as new as industrial security. In this chapter conclusions will be presented followed by a discussion of problem areas that need additional study.

I. CONCLUSIONS

Intrusion detection and/or closed circuit television equipment can be used to increase the effectiveness of a guard force. It will not inevitably increase the effectiveness, but with proper planning, selection of equipment, and employment, increased effectiveness may be achieved.

In the opinion of the security directors interviewed, this increased effectiveness may permit reduction of the total strength of the guard force. Such reduction may be accomplished without reducing the level of security provided. As pointed out earlier, it was not possible in this study to provide an objective and reliable test of this opinion. The fact that all security directors interviewed indicated that if they could "start from scratch" with their security system they would not make any changes indicates that they are not willing to admit that they have erred. Such an attitude raises serious questions concerning the reliability of their opinions concerning relative security provided. The government inspectors involved are placed in a similar position. They have approved the use of the equipment to supplant manpower and would be forced to admit that they were in error if they failed to agree with the opinion of the security directors on relative level of security provided.

The proposed hypothesis that use of the equipment may permit management to redistribute manpower to provide additional services or security could not be tested because none of the firms studied would admit that this had been done or would be done if possible. It was obvious, however, that this was sometimes the case. As an example, one security director stated that if the equipment replaced guards they would not be released but rather the reduction in the guard force would be accomplished through attrition.

Obviously these surplus men would be used to provide some type of additional security or service until the guard force was reduced to its "proper" strength.

As pointed out earlier, it is felt that the best indication of possible monetary savings was obtained by asking security directors how many security guards would be required to maintain the same level of security if they were forced to discontinue use of closed circuit television and/or intrusion detection equipment. This theoretical increase in manpower cost was then compared with the total cost of using the equipment. Assuming the number of additional guards indicated was correct, the theoretical savings for six of the firms studied would be substantial. Comparative monetary savings for each facility studied based on this theoretical situation were presented on page 100 in the Analysis Chapter.

In future studies concerning the effect of use of intrusion detection equipment and/or closed circuit television on guard force personnel requirements researchers should not attempt to study this equipment as a separate entity. Most security directors apparently think of automatic fire protection equipment, intrusion detection and closed circuit television equipment, and in some cases, industrial monitoring equipment, as a single facet of a security system. It is recommended that future studies be so oriented.

In the present project a great deal of effort was devoted to preparation of the descriptive portion of the study. It is felt that this is important because such a study had not been previously completed. Perhaps future researchers with this information and with the knowledge of the limiting factors encountered in this study can formulate a methodology which will be more fruitful.

II. PROBLEM AREAS WHICH NEED ADDITIONAL STUDY

In conducting this study several areas were identified which need additional investigation. Some are directly related to use of intrusion detection and closed circuit television equipment. Others are indirectly related to such equipment.

One area is the use of contract security guards as opposed to hiring company guards. Although not brought out directly in the interviews, varying opinions were expressed by security directors on the advantages and disadvantages of each. Some would not consider using contract guards under any circumstances while others felt that large monetary savings are possible without a loss of effectiveness.

Another area which could be profitably explored is a comparison of leasing closed circuit television and intrusion detection equipment with outright purchase of such equipment. One prominent security director of a large

corporation that is well known in this area for efficient security operations felt that it is advantageous to lease the equipment. He pointed out that firms that lease equipment are able to use the latest equipment and will not be "stuck" with obsolete devices when better models are introduced. Another advantage to most firms is a corporate tax savings which result from leasing equipment. Under the present tax structure the fee for leasing equipment is chargeable as a business expense while a purchase is considered a capital investment. The dollars spent for leased equipment would in effect be "worth less" than dollars spent on purchased equipment. Leasing might, therefore, be less expensive than buying the equipment.

Additional study is needed to determine factors which should be considered in making a decision on whether or not to use intrusion detection and/or closed circuit television equipment. One of these factors might be the effect of use of the equipment on employee morale, particularly members of the guard force, to determine if the possible monetary savings justifies the adverse effect on morale. Another factor which might be considered is the effect of reduced guard force manpower on disaster plans and procedures. Closed circuit television and intrusion detection equipment may provide protection for an area but machines cannot exercise judgment, assume control of a situation, render first aid, etc., in cases of emergency.

A study should be conducted to determine the effect that competition between industrial firms has on the free flow of information on industrial security techniques and procedures. As pointed out earlier, some security directors actively attempt to keep this information from their competitors. Some method needs to be developed to combat this situation which retards the development of industrial security as a true profession.

BIBLIOGRAPHY

Books

Davis, John R. Industrial Plant Protection. Springfield, Illinois: Charles C. Thomas, Publisher, 1957.

McGhee, H. A. Industrial Television. London: Wyman and Sons, Ltd., 1957.

Mayers, M. A., and Chipp, R. D. Closed Circuit Television System Planning. New York: John F. Rider, Publisher, 1957.

Noll, E. M. Closed-Circuit and Industrial Television. New York: Macmillan Co., 1956.

Zworykin, V. K., E. G. Ramberg, and L. E. Flory. Television in Science and Industry. New York: John Wiley and Sons, 1958.

Publications of Government and Other Organizations

Allen B. DuMont Laboratories, Inc. Industrial Television Handbook. New Jersey: George R. Epple Company, 1958.

American District Telegraph Company. Protecting Life, Property and Profits. New York: American District Telegraph Company, 1959.

American District Telegraph Company. Electric Protection Services, Book II. New York: American District Telegraph Company, 1960.

American District Telegraph Company. Proprietary Systems and Their Role in Plant Security. New York: American District Telegraph Company, undated.

Bagno, Sam, J. B. Cooper, and E. I. Levy. "The Ultrasonic Burglar System," IRE Convention Record, Part 6, Audio and Ultrasonics. New York: Institute of Radio Engineers, 1954.

Department of Army. Intrusion Detection Devices, TB PMG 26. Washington: Government Printing Office, June, 1959.

Department of Army. Intrusion Detection Systems, ORDM 10-2. Washington: Government Printing Office, May, 1961.

Department of Army. Physical Security Standards, ORDM 10-3. Washington: Government Printing Office, May, 1961.

Department of Commerce. The U.S. Industrial Outlook for 1960. Washington: Government Printing Office, 1959.

Department of Commerce. The U.S. Industrial Outlook for 1961. Washington: Government Printing Office, 1960.

Department of Commerce. The U.S. Industrial Outlook for 1962. Washington: Government Printing Office, 1961.

Department of Defense. Standards for Plant Protection. Washington: Government Printing Office, 1952.

Department of Defense. Industrial Security Manual for Safeguarding Classified Information. Washington: Government Printing Office, November, 1961.

Gaston, Edward F. Automation of Property Protection. New York: American District Telegraph Company, undated.

Minneapolis-Honeywell Company. Security and Equipment Surveillance Systems. Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated.

Minneapolis-Honeywell Company. Secret Sentry, W614. Minneapolis, Minnesota: Minneapolis-Honeywell Company, undated.

Mosler Research Products, Incorporated. Electronic Anti-intrusion Systems and Electronic Investigative Equipment. Danbury, Connecticut: Mosler Research Products, Incorporated, undated.

National Petroleum Council. Security Principles for the Petroleum and Gas Industries. Washington: National Petroleum Council, May, 1955.

Office of Defense Mobilization. Standards for Physical Security of Industrial and Governmental Facilities. Washington: Government Printing Office, 1958.

Powers Regulator Company. Introduction to Security Systems. Skokie, Illinois: Powers Regulator Company, 1961.

Powers Regulator Company. AL-15 Radi-Matic Barrier. Skokie, Illinois: Powers Regulator Company, 1960.

RCA Service Company. Closed-circuit Television Systems. Camden, New Jersey: RCA Service Company, 1958.

Underwriters' Laboratories. Standards for Safety; Installation, Classification and Certification of Burglar Alarm Systems, UL 681. Chicago: Underwriters' Laboratories, February, 1959 (as revised to May, 1961).

Underwriters' Laboratories. Testing for Safety. Chicago: Underwriters' Laboratories, 1959.

Underwriters' Laboratories. Accident, Automotive, and Burglary Protection Equipment Lists. Chicago: Underwriters' Laboratories, September, 1962.

Underwriters' Laboratories. 1961 Field Service Record, Certificated Burglar Alarms, Bulletin Number 22. Chicago: Underwriters' Laboratory, April, 1962.

U.S. Army Intelligence School. Electrical Protective Systems; Supplemental Reading Number 30612. Ft. Holabird, Maryland: U.S. Army Intelligence School, 1962 (Mimeographed).

Worner Electronic Devices. Fotolectric Systems. Rankin, Illinois: Worner Electronic Devices, 1962.

Periodicals

Achilli, E. R. "Revolutionary New Burglar Alarm System, Sonic Guard Designed to Reduce Losses," Weekly Underwriter, CLXVIII (June 6, 1953), 1556.

"Alarms and Incursions," Economist, CXCIX (June 3, 1961), 1019-20.

Anderson, J. C., and T. Winer. "Temperature-Stabilized Photo-Transistor Relay Circuit," Electronic Engineering, XXXI (January, 1959), 36-37.

Anderson, K. "Why Burglars Can't Win," Popular Mechanics, CIX (February, 1958), 134-37.

"An Electrical Alarm--Matting," Scientific American, LXXX (March 18, 1899), 165.

"An Electric Burglar Alarm for Safes," Scientific American, LXXI (December 22, 1894), 395.

"An Annunciator for Burglar Alarms," Scientific American, LXV (November 14, 1891), 306.

"A Novel Burglar Alarm," Scientific American, LXXVII (September 18, 1897), 180.

"A Simple Burglar Alarm," Scientific American, XCI (December 10, 1904), 408.

"At Home: No Unauthorized Entry," Engineering, CXCIII (January 19, 1962), 120.

"Automate Plant Protection," Factory, CXIX (December, 1961), 60.

"Babaco Alarm Systems Completes 25 Years of Theft Protection," Weekly Underwriter, CLXXIV (May 5, 1956), 1058.

Bagno, Sam. "Sensitive Capacitance Intruder Alarm," Electronics, XXXIII (September 16, 1960), 65-7.

Bagno, Sam. "Designing Ultrasonic Alarm Systems: Doppler Effect Detection System," Electronics, XXVIII (August, 1955), 106-11.

Bagno, Sam, and Fasal, J. "Intruder Alarm Uses Phase-sensitive Detector," Electronics, XXXI (February 14, 1958), 102-5.

"Beating Burglars with Black Light," Popular Mechanics, LXIX (April, 1938), 514-517.

"Big Brother Is Listening," Mill and Factory, LXII (February, 1958), 91.

Black, D. "Invisible War on Crime," Popular Mechanics, LIX (February, 1933), 218-221.

Browning, G. H. "Balanced-Capacitance Fence Alarm System," Electronics, XXIX (April, 1956), 150-52.

Buckley, John L. "Industrial Security and Plant Engineering," Plant Engineering, XVI (February, 1962), 115-118.

"Burglar Alarm Systems Prevent Truck Cargo Thefts; Air Freight Thefts," Weekly Underwriter, CLXXIII (October 8, 1955), 820.

"Burglar Trap of Black Light," Architectural Record, LXXXI (May, 1937), 49.

"Burglary Underwriters and Inspectors Conference," National Underwriters, LIX (December 29, 1955), 15.

Burns, W. J. "How Safe Is Your Home?," Popular Mechanics, LVII (May, 1932), 772-777.

Caffrey, James J. "Frequency of Burglaries Differs Considerably from City to City," The National Underwriter, LXV (August 18, 1961), 10.

Caringella, C. "Build an Infrared Burglar Alarm," Popular Electronics, XIV (February, 1961), 46-9.

Carroll, E. C. "Closed Circuit Television for Industrial Applications," Iron and Steel Engineer, XXXVII (July, 1960), 78.

Carter, J. B. "Radio Burglar Alarm Built with Receiver Parts," Popular Science, CXXVIII (January, 1936), 52-53.

Clark, B. "Bad News for Burglars," Banking, VL (June, 1953), 54.

"Closed Circuit TV Guards Philadelphia Garage," American City, LXXVII (June, 1962), 123.

"Closed Circuit Television Guards Turnstiles," Electronics XXX (August 1, 1957), 26.

"Closed Circuit Television Is Growing More Versatile," Barrons, XXXIX (September 7, 1959), 5.

"Crime in U.S. Hits New Peak," ADT Transmitter, XXXIV (September-October, 1962), 2.

Crowley, C. A. "Clocks Control Burglar Alarms," Popular Mechanics, LXXVIII (August, 1942), 133-136.

"Electronic Alarm," Scientific American, CLXXVI (April, 1947), 176.

"Electronic 'Curtains' Curtail Convicts," ADT Transmitter, XXXIV (July-August, 1962), 7.

Forbin, J. C. "Alarm System that Protects 16 Ways," Factory, CXII (October, 1954), 140-44.

Fox, F. L. "Putting the Burglar in Jeopardy," Technical World, XX (October, 1913), 276-282.

Gorman, R. "War Between Burglars and Inventors," Popular Science, CLXXVI (April, 1960), 91-4.

Gustafson, P. "These Safecrackers Can Get Away with It," Popular Science, CLII (March, 1948), 113-118.

"Hinge Connection for Electric Burglar Alarms," Scientific American, LXII (June 7, 1890), 363.

Howard, J. H. "Electric Protection for Banks," Scientific American, LXXIX (August 20, 1898), 117.

"How Dayton Minimizes Vandalism Losses," American School Board Journal, CXL (May, 1960), 48.

"How to Booby Trap a Burglar," Good Housekeeping, CLI (November, 1960), 152.

Hyde, R. K. "Automatic Industrial Baby-Sitting," Spectator, CLXIV (September, 1956), 30-1.

"Industrial Photo Electric Equipment," Mass Production, XXVII (January, 1951), 56-71.

"Industrial TV: More Than Novelty, Not Yet a Full Success," Business Week, no vol. # (September 14, 1957), 106.

"Intruder Alarm Market Up," Electronics, XXX (April 10, 1957), 30.

"Invisible Light Rays Guard Treasures and Art," Popular Mechanics, LIX (April, 1933), 556-557.

Ives, R. L. "Prowler Alarm," Popular Mechanics, CXVI (February, 1961), 136-7.

Jackson, C. E. "Intrusion Alarms," Radio News, XXX (May, 1943), 14-16.

Kempner, Stanley. "Ultrasonic System Detects Intruders," Electronics, XXV (April, 1952), 104-5.

Lindsay, Maxwell H. A. "Electronic Protective Systems," Electrical Engineering, LXIII (October, 1944), 367.

Lindsay, Maxwell H. A. "ADT Takes a Giant Step," The ADT Transmitter, XXIV (May-June, 1962), 7.

"Loudspeaker Burglar Alarm," Science, LXXXIII (March 20, 1936), sup. 9-10.

Lynch, T. L. "Commends Alarm System; Aided Loss Prevention Efforts," Eastern Underwriter, LIV (September 18, 1953), 35.

McLucas, J. L., and Laughlin, R. D. "Moving Target Detection," Electronics, XXVII (August, 1954), 169-71.

McRoberts, J. A. "Silent Sentinel: Novel Frequency Shift Alarm," Popular Mechanics, CVII (May, 1957), 217-220.

Malone, Lee F. "Control of Closed Areas by Closed Circuit Television," Industrial Security, II (April, 1958), 8.

Malone, Lee F. "Modern Electronics Assisted by the Age Old Mirror," Industrial Security, VII (January, 1963), 12.

Miller, J. N. "Pity the Poor Burglar," The Reader's Digest, LXXX (November, 1962), 207-8.

Murphy, Thomas J. "The Capacity Alarm Comes of Age," Signal, VI (February, 1960), 8.

"New Babaco Burglar Alarm System for Pick Up and Delivery Trucks," Weekly Underwriter, CLXXII (January 22, 1955), 248.

"New Burglar Alarms for Trucks Can Be Purchased Outright," Fleet Owner, LIII (July, 1958), 155.

"Newest Roof-Fire Watchman for Remote Control TV," Factory, CXIV (March, 1956), 91.

"New Swiss Burglar Alarm Operates Like Seismograph," Science Newsletter, XL (August 23, 1941), 41.

"New Twists: Ultrasonic Burglar Alarm System," Nation's Business, XLIII (April, 1955), 101.

Pearce, G. P. "Burglar and Safe Maker; Electrical Guard," Scientific American, Supplement, LXVI (November 14, 1908), 310.

"Phantom Gateman Operates Via TV," Factory, CXIX (June, 1961), 170.

"Radio Device Detects Intruders," Aviation Week, LXXI (July 20, 1959), 61.

"Robot Guardians of Billions," Popular Mechanics, LXXIX (February, 1943), 28-31.

Rochette, Walter L. "Closed Circuit Television; New View for Business," Personnel Journal, XXXIX (March, 1961), 409-412.

"Safe as a Bank Vault," Factory, CXIV (June, 1956), 95.

"Saving Big with Robot Guards," Factory, CXV (May, 1957), 74.

Scott, H. P. "Lighting and Protection for Art Museum," Electrical Construction and Maintenance, LV (March, 1956), 76-83.

Smith, E. H. "The Burglar and the Alarm," Scientific American, CXXVIII (May, 1923), 294-295.

"Sound Guards Secrets; Ultrasonic Intruder Detection Alarm," Science Newsletter, LXXIII (May 10, 1958), 294.

Stieglitz, L. "Burglar Alarm Protection Highly Important in Underwriting," Eastern Underwriter, LV (29 January, 1954), 27.

Stimson, T. E. "Don't Be Caught Napping," Popular Mechanics, XCI (February, 1959), 198-199.

Sugar, M. "Watchdog Television Security System Demonstrated," Electrical Engineering, LXXX (September, 1961), 735.

"The Attack on Plant Protection," Factory, CXIX (November, 1961).

"The Domestic Telegraph," Scientific American, XXVII (July 20, 1872), 39.

"The Electric Burglar Alarm," Popular Science, XVIII (November, 1880), 56.

"This Fire and Burglar Alarm Is Fool Proof," Popular Mechanics, LX (September, 1933), 450-454.

Turner, R. P. "Crime Detection; Electronic Devices," Radio News, XXX (September, 1943), 21-22.

"TV Camera Guard for Garage Doors Provides Low Cost Plant Security," Gas Age, CXIX (November 23, 1961), 10-11.

"TV for Industry--Uses Unlimited," Steel, CVL (October, 1959), 64-65.

"TV Goes on Guard for Esso," Oil and Gas Journal, LV (March 18, 1957), 98.

"TV Guards Power Plant Gate for Louisiana Power and Light Company," Electrical World, CVL (January 30, 1956), 48-49.

"TV Stands Guard; Used to Monitor Employee Entrance at the Baton Rouge Refinery," Petroleum Refiner, XXXVI (May, 1957), 254.

"Twenty Acres of Field Testing Facilities," ADT Transmitter, XXXII (December, 1960), 7.

"Ultrasonic Alarm: Alertonic," Time, LXII (October 26, 1953), 91.

"Ultrasonic Alarm Detects Burglars with Doppler," Machine Design, XXXIV (May 10, 1962), 138-139.

"Ultrasonic Burglar Alarm, Readied by Walter Kidde and Company," National Underwriter, LVIII (July 22, 1954), 23.

"Urges Cooperation Between Insurers and Alarm Makers to Cut Burglaries," National Underwriters, XL (August 16, 1956), 28.

Winner, L. "Two Tube Capacity-operated Burglar Alarm," Popular Mechanics, LXVI (August, 1936), 260.

"Wireless Burglar Alarm for Safes," Scientific American, XCI (December 24, 1904), 459.

Wiren, S. "Intrusion Detection by Electromagnetic Fields," Siemen's Review, XXVIII (October, 1961), 341-44.

Unpublished Materials

American District Telegraph Company. Letter from Mr. G. G. N. Purcell, Public Relations Department, dated March 29, 1963.

United States Army Supply and Maintenance Command. Letter from Chief, Security Division, dated January 10, 1963.

APPENDIX A

SAMPLE INTERVIEW SCHEDULE

1. Facility code letter _____.

   Time and date of interview _____.

2. What is the general nature of the business of your firm?

COMMENT: I would like to obtain information on specific facilities in the Wayne County area in which closed circuit television and/or intrusion detection equipment is used. (Allow time for interviewee to identify such a facility mentally, then continue.)

3. What is this facility used for?

4. What general types of closed circuit television and/or intrusion detection equipment is used there?

5. What is the primary purpose of the security system?

6. Is the equipment used to protect open areas or buildings?

7. What is the approximate size of the protected area?

8. Was the equipment leased or purchased?

   (a) Costs for facilities using purchased equipment:

      (1) What was the initial cost of the equipment?

      (2) What was the cost of installation?

      (3) What is the annual maintenance cost?

      (4) What is the annual depreciation cost (initial cost divided by life expectancy of the equipment)?

(b) Costs for facilities using leased equipment:

(1) What was the installation cost?

(2) What is the annual leasing fee?

9. Does use of the equipment increase the effectiveness of your guard force?

10. What is the average annual cost of one security guard (including all costs; wages, fringe benefits, equipment, etc.)?

11. Was the equipment installed before or after the guard force was operational?

SECTION B (Use when equipment was installed after the guard force was operational.)

Were you able to reduce the total strength of your guard force at this facility through use of the equipment without reducing the level of security provided?

NOTE: Now skip to section D.

SECTION C (Use when equipment was installed before the guard force was operational.)

Would more men have been required to achieve the same level of security if the equipment had not been used? If so, how many?

SECTION D

1. If you were forced to discontinue use of the equipment and were required to maintain the same level of security, what effect would this have on the total strength of your security guard force?

2. Have any attempts been made to breach the system? If so, were they successful?

3. If you could "start from scratch" with your security system for this facility, what changes would you make?

APPENDIX B

RECAPITULATION OF RESPONSES TO INTERVIEW QUESTIONS

SECTION A

1. Facility code letter with time and date of interview:

FACILITY	TIME AND DATE OF INTERVIEW
A	9:00 a.m., June 11, 1963
B	2:00 p.m., June 11, 1963
C	4:00 p.m., June 11, 1963
D	10:00 a.m., June 12, 1963
E	9:00 a.m., June 13, 1963
F	2:00 p.m., June 13, 1963
G	2:00 p.m., June 14, 1963

2. What is the general nature of the business of your firm?

A. Business machine manufacturer.

B. Automobile manufacturer.

C. Automobile manufacturer.

D. Business machine manufacturer.

E. Manufacturer of product for personal consumption (interviewee requested that identification be made in this manner).

F. Cutting tool manufacturer.

G. Automobile manufacturer.

3. What is this facility used for?

A. Production.

B. Production of automobile parts.

C. Storage of automobile parts.

D. Production.

E. Research and production.

F. Production.

G. Storage of automobile parts.

4. What general types of closed circuit television and/or intrusion detection equipment is used there?

A. A closed circuit system with four cameras and four monitors. The system includes an audio detection system to draw the attention of the guard observing the monitors to the proper area.

B. Electromechanical devices on all openings augmented by photoelectric detectors.

C. Electromechanical devices on all openings augmented by photoelectric detectors.

D. A closed circuit television system with one camera and a single monitor with audio detectors in the protected area to draw the attention of the guard to the monitor.

E. Electromechanical devices on all openings.

F. Electromechanical devices on all openings.

G. Electromechanical devices on all openings augmented by photoelectric detectors.

5. What is the primary purpose of the security system?

A. To meet security requirements for a classified government contract.

B. To prevent theft and vandalism.

C. To prevent thefts.

D. To meet security requirements for a classified government contract.

E. To protect against industrial espionage, theft, and to meet insurance standards.

F. To meet recommended government security standards and to prevent thefts.

G. To prevent thefts.

6. Is the equipment used to protect open areas or buildings?

A. Buildings.

B. Buildings.

C. Buildings.

D. Buildings.

E. Buildings.

F. Buildings.

G. Buildings.

7. What is the approximate size of the protected area?

A. Four large rooms of approximately 20,000 square feet each.

B. Approximately 150,000 square feet.

C. Approximately 450,000 square feet.

D. Approximately 50,000 square feet.

E. Buildings covering about six city blocks.

F. Approximately 20,000 square feet.

G. Approximately 200,000 square feet.

8. Was the equipment leased or purchased?

A. Purchased.

B. Leased.

C. Leased.

D. Purchased.

E. Leased.

F. Leased.

G. Leased.

(a) Costs for facilities using purchased equipment:

(1) Initial cost of equipment?

A -- $11,000.00.

D -- $6,000 including installation.

(2) Installation cost?

A -- $500.00.

D -- Included in initial cost of the equipment.

(3) Annual maintenance cost?

A -- $500.00.

D -- New installation, estimated at $150.00.

(4) Depreciation (Initial cost of equipment divided by life expectancy of equipment).

A -- $1,100 per year.

D -- $300.00 per year.

(b) Costs for facilities using leased equipment?

(1) Installation cost?

B -- $15,000.00 (Includes automatic fire protection equipment).

C -- $15,000.00 (Includes automatic fire protection equipment).

E -- $35,000.00.

F -- No cost involved, was installed when the building was leased.

G -- $4,500.00.

(2) Annual leasing fee?

B -- $1,500.00 (Includes automatic fire protection equipment).

C -- $1,500.00 (Includes automatic fire protection equipment).

E -- $10,000.00.

F -- $1,100.00.

G -- $4,000.00.

9. Does use of the equipment increase the effectiveness of your guard force?

A. Yes.

B. Yes, it actually eliminated the need for on-site guards when combined with automatic fire protection equipment and industrial monitoring devices.

C. Yes, it actually eliminated the need for on-site guards when combined with automatic fire protection equipment.

D. Yes.

E. Yes.

F. Yes, it eliminated the need for on-site guards.

G. Yes, it eliminated the need for on-site guards.

10. What is the average annual cost of one security guard (including all costs; wages, fringe benefits, equipment, etc.)?

A. $7,000.00.

B. $8,000.00 if we hire him or about $5,000.00 if a contract guard service is used.

C. $8,000.00 if we hire him or about $5,000.00 if a contract guard service is used.

D. $7,000.00.

E. $8,000.00.

F. No experience with guards so it is hard to estimate, would cost at least $3,000.00.

G. $7,000.00.

11. Was the equipment installed before or after the guard force was operational?

A. After.

B. Before.

C. After.

D. After.

E. After.

F. Before.

G. Before.

SECTION B (When equipment was installed after the guard force was operational).

1. Were you able to reduce the total strength of your guard force at this facility through use of the equipment without reducing the level of security provided?

A. No reduction but the equipment was added when security was greatly increased in order to qualify for a classified government contract and prevented us from having to add nine additional guards.

C. Yes, but the fire protection and intrusion detection equipment cannot be considered separately. If automatic fire protection equipment had not been installed with the intrusion detection equipment the guard force could not be reduced.

D. No reduction but it kept us from adding three additional men to the guard force.

E. A reduction was made in the guard force but it was not due to the intrusion detection equipment. It was due to installation of automatic fire protection equipment which was installed with the intrusion detection equipment. Based on experience no reduction of the guard force could be made if the intrusion detection equipment was removed.

SECTION C (When equipment was installed before the guard force was operational).

1. Would more men have been required to achieve the same level of security if the equipment had not been used? How many?

B. Yes, three men.

F. Yes, two men.

G. Yes, two men.

SECTION D

1. If you were forced to discontinue use of the intrusion detection equipment and/or intrusion detection equipment and were required to maintain the same level of security, what effect would this have on the total strength of the security guard force?

A. Would have to add nine men.

B. Would have to add three men.

C. Would have to add three men.

D. Would have to add three men.

E. None.

F. Would have to add two men.

G. Would have to add two men.

2. Have any attempts been made to breach the system? If so, were they successful?

A. Yes, but none have been successful.

B. No.

C. No.

D. Yes, none have been successful.

E. No.

F. No.

G. No, not at this particular facility but similar buildings have been successfully entered without detection. It is not economically feasible to have complete protection for such areas.

3. If you could "start from scratch" on your security system for this facility, what changes would you make?

A. None.

B. None.

C. None.

D. None.

E. None.

F. None.

G. None.