UFC 4-020-04A
1 MARCH 2005
Change 2 – 22 September 2009

UNIFIED FACILITIES CRITERIA (UFC)

ELECTRONIC SECURITY SYSTEMS: SECURITY ENGINEERING

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

UFC 4-020-04A
1 MARCH 2005
Change 2 – 22 September 2009

UNIFIED FACILITIES CRITERIA (UFC)

SECURITY ENGINEERING: ELECTRONIC SECURITY SYSTEMS

U.S. ARMY CORPS OF ENGINEERS (Preparing Activity)

Record of Changes (changes are indicated by **\1** ... /**1**/)

Change No.	Date	Location
1	June 2006	Forward changed.
2	Sep 22 2009	Removed “F” from document number

This UFC supersedes TM 5-853-4, dated 12 May 1994. The format of this UFC does not conform to UFC 1-300-01; however, the format will be adjusted to conform at the next revision. The body of this UFC is a document of a different number.

FOREWORD

\1\
The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with USD(AT&L) Memorandum dated 29 May 2002. UFC will be used for all DoD projects and work for other customers where appropriate. All construction outside of the United States is also governed by Status of Forces Agreements (SOFA), Host Nation Funded Construction Agreements (HNFA), and in some instances, Bilateral Infrastructure Agreements (BIA.) Therefore, the acquisition team must ensure compliance with the more stringent of the UFC, the SOFA, the HNFA, and the BIA, as applicable.

UFC are living documents and will be periodically reviewed, updated, and made available to users as part of the Services' responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC), and Air Force Center for Engineering and the Environment (AFCEE) are responsible for administration of the UFC system. Defense agencies should contact the preparing service for document interpretation and improvements. Technical content of UFC is the responsibility of the cognizant DoD working group. Recommended changes with supporting rationale should be sent to the respective service proponent office by the following electronic form: Criteria Change Request (CCR). The form is also accessible from the Internet sites listed below.

UFC are effective upon issuance and are distributed only in electronic media from the following source:

- Whole Building Design Guide web site http://dod.wbdg.org/.

Hard copies of UFC printed from electronic media should be checked against the current electronic version prior to use to ensure that they are current. /1/

AUTHORIZED BY:

DONALD L. BASHAM, P.E.
Chief, Engineering and Construction Division
U.S. Army Corps of Engineers

James Wright

_
DR. JAMES W WRIGHT, P.E.
Chief Engineer
Naval Facilities Engineering Command

Kathleen I. Ferguson

KATHLEEN I. FERGUSON, P.E.
The Deputy Civil Engineer
DCS/Installations & Logistics
Department of the Air Force

_
Dr. GET W. MOY, P.E.
Director, Installations Requirements and
Management
Office of the Deputy Under Secretary of
Defense
(Installations and Environment)

ARMY TM 5-853-4

TECHNICAL MANUAL

SECURITY ENGINEERING ELECTRONIC SECURITY SYSTEMS

Approved for public release; Distribution is unlimited

HEADQUARTERS, DEPARTMENT OF THE ARMY
12 MAY 1994

REPRODUCTION AUTHORIZATION/RESTRICTIONS

TECHNICAL MANUAL
No. 5-853-4

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, DC, *12 May 1994*

SECURITY ENGINEERING
ELECTRONIC SECURITY SYSTEMS

			Paragraph	Page
CHAPTER	1.	INTRODUCTION		
		Purpose	1-1	1-1
		Scope	1-2	1-1
		References	1-3	1-1
		Definition	1-4	1-1
		Codes, Standards, and Regulations	1-5	1-1
		Regulatory Requirements	1-6	1-1
		Use of Electronic Security Systems	1-7	1-2
		Interior Electronic Security Systems	1-8	1-2
		Exterior Electronic Security Systems	1-9	1-2
		Data Transmission	1-10	1-2
		State-of-the-Art	1-11	1-2
		Reliability and Availability	1-12	1-2
		Expansion	1-13	1-2
		Functional Equivalency	1-14	1-2
		Designer's Responsibility	1-15	1-3
	2.	THREATS AND ASSETS		
		General	2-1	2-1
		Threat Definition	2-2	2-1
		Asset Description	2-3	2-1
	3.	SYSTEMS DESCRIPTIONS		
Section	I.	CONFIGURATIONS		
		General	3-1	3-1
		IDS Components	3-2	3-1
		CCTV Components	3-3	3-2
		EECS Components	3-4	3-4
	II.	STANDARD MILITARY SYSTEMS		
		Objective	3-5	3-5
		J-SIIDS	3-6	3-5
		BISS	3-7	3-5
		REMBASS	3-8	3-5
		FIEPSS	3-9	3-5
		ICIDS	3-10	3-5
	III.	SECURITY CENTER EQUIPMENT		
		Security Center Area	3-11	3-6
		Console Consideration	3-12	3-7
		Room Layout	3-13	3-8
		Other Considerations	3-14	3-9
	IV.	GROUNDING, SHIELDING, AND TRANSIENT PROTECTION		
		Types of Interference	3-15	3-9
		Transient Protection Devices	3-16	3-9
		Grounding	3-17	3-9
		Shielding	3-18	3-10
	4.	INTERIOR INTRUSION DETECTION SENSORS		
	I.	TYPES OF SENSORS		
		General	4-1	4-1
		Sensor Terminology	4-2	4-1
		Boundary Penetration Sensors	4-3	4-2
		Volumetric Motion Sensors	4-4	4-5
		Point Sensors	4-5	4-9
		Duress Alarm Devices	4-6	4-9
	II.	DESIGN GUIDELINES		
		Basic Design Criteria	4-7	4-10
		Layout of Boundary Penetration Sensors	4-8	4-12
		Layout of Volumetric Motion Sensors	4-9	4-13

Approved for public release; Distribution is unlimited

			Paragraph	Page
		Layout of Point Sensors	4-10	4-18
		Additional Sensor Considerations	4-11	4-18
CHAPTER	5.	EXTERIOR INTRUSION DETECTION SENSORS		
Section	I.	TYPES OF SENSORS		
		General	5-1	5-1
		Fence Sensors	5-2	5-1
		Buried Line Sensors	5-3	5-5
		Line-of-Sight Sensors	5-4	5-6
		Video Motion Sensors	5-5	5-6
	II.	DESIGN GUIDELINES		
		Basic Design Criteria	5-6	5-6
		Perimeter Layout and Zoning	5-7	5-9
		Fence Sensor Design	5-8	5-11
		Buried Line Sensor Design	5-9	5-12
		Line-of-Sight Sensor Design	5-10	5-13
		Other Considerations	5-11	5-16
	6.	IDS ALARM ANNUNCIATION SYSTEM		
	I.	HARDWARE		
		IDS Alarm Annunciation	6-1	6-1
		IDS Alarm Annunciation Configuration	6-2	6-1
		Data Storage	6-3	6-1
		Operator Interfaces	6-4	6-3
		IDS Field Data Collection	6-5	6-4
		DTM	6-6	6-5
		CCTV Interface	6-7	6-5
		EECS Interface	6-8	6-5
	II.	SOFTWARE		
		Types of Software	6-9	6-7
		Software Functions	6-10	6-7
		CCTV Interface	6-11	6-8
		EECS Interface	6-12	6-8
	III	RELIABILITY		
		Reliability Considerations	6-13	6-8
	7	ELECTRONIC ENTRY CONTROL		
	I.	TYPES OF ENTRY CONTROL DEVICES		
		General	7-1	7-1
		Coded Devices	7-2	7-1
		Credential Devices	7-3	7-1
		Biometric Devices	7-4	7-3
		Device Combinations	7-5	7-4
	II.	APPLICATION GUIDELINES		
		Site Specific Factors	7-6	7-4
		Automated Entry Control System Functions	7-7	7-4
		Performance Criteria	7-8	7-6
		Coded Device Considerations	7-9	7-6
		Credential Device Considerations	7-10	7-7
		Biometric Device Considerations	7-11	7-8
		Command and Control	7-12	7-9
		Economic Considerations	7-13	7-11
	III.	DESIGN GUIDELINES		
		Basic Design Criteria	7-14	7-12
		Equipment Layout and Protection	7-15	7-12
		Other Considerations	7-16	7-13
	8.	CCTV FOR ALARM ASSESSMENT AND SURVEILLANCE		
	I	ELEMENTS OF A CCTV SYSTEM		
		General	8-1	8-1
		CCTV Camera Components	8-2	8-1
		Video Signal and Control Links	8-3	8-5
		CCTV System Synchronization	8-4	8-6
		Video Processing and Display Components	8-5	8-6
	II.	APPLICATION GUIDELINES		
		Site Specific Factors	8-6	8-8
		Performance Criteria	8-7	8-8

			Paragraph	Page
		Lighting and Imaging Considerations	8-8	8-10
		Economic Considerations	8-9	8-11
	III.	DESIGN GUIDELINES		
		System Familiarity	8-10	8-15
		CCTV Camera Placement and Lighting	8-11	8-15
		Layout Considerations	8-12	8-16
		Camera Placement Procedure and Formulas	8-13	8-16
		CCTV System Interfaces	8-14	8-18
CHAPTER	9.	DATA TRANSMISSION		
		General	9-1	9-1
		Data Transmission Media	9-2	9-1
		Data Transmission Techniques	9-3	9-2
		Data Transmission Hardware	9-4	9-2
		Data Transmission Security	9-5	9-2
		Additional Considerations	9-6	9-3
	10.	INTERFACES		
		General	10-1	10-1
		Electrical	10-2	10-1
		Civil	10-3	10-1
		Mechanical	10-4	10-2
		Structural	10-5	10-2
		Architecture	10-6	10-2
		Other Interfaces	10-7	10-3
		Health/Safety and Fire	10-8	10-3
		Operations	10-9	10-3
	11.	PROJECT IMPLEMENTATION		
	I.	DESIGN CONSIDERATIONS		
		General	11-1	11-1
		Basic Guidance	11-2	11-1
		Electronic Security Systems Effectiveness	11-3	11-1
		Interior IDS Considerations	11-4	11-3
		Exterior IDS Considerations	11-5	11-4
		Physical Considerations	11-6	11-4
	II.	DESIGN METHODOLOGY		
		Design Sequence	11-7	11-4
		Preparation of Design Criteria	11-8	11-4
		Design Kickoff Meeting	11-9	11-5
		Design Criteria Validation	11-10	11-5
		Concept Design	11-11	11-6
		Final Design	11-12	11-6
		Procurement and Contract Award	11-13	11-6
APPENDIX	A.	REFERENCES		A-1
	B.	FACILITY SECURITY LEVEL AND IDS REQUIREMENTS		B-1
	C.	SURVEY PROCEDURES FOR ELECTRONIC SECURITY SYSTEMS		C-1
BIBLIOGRAPHY				Biblio-1
GLOSSARY				Glossary-1

List of Figures

Figure	Title	Page
3-1	Typical IDS Configuration	3-2
3-2	Typical CCTV System	3-3
3-3	Typical EECS System	3-4
3-4	Typical Security Center Layout	3-6
3-5	Typical Security Console Layout	3-8
4-1	Wall-Mounted Structural Vibration Sensors	4-2
4-2	Typical Passive Ultrasonic Sensor Detection Pattern	4-3
4-3	BMS Mounting Configurations	4-4
4-4	Photoelectric Beam Sensor Configurations	4-5
4-5	Typical Ultrasonic Motion Sensor Beam Patterns	4-6
4-6	Typical Detection Patterns for Microwave Motion Sensors	4-7
4-7	Typical Detection Patterns for a Passive Infrared Motion Detector	4-8
4-8	Capacitance Proximity Sensor Application	4-10
4-9	Layered IDS Detection	4-11

Figure Title Page
4-10 Installation Using a Lattice for Vibration Sensors 4-12
4-11 Typical Balanced Magnetic Switch Installation 4-13
4-12 Placement of Ultrasonic Transceivers 4-15
4-13 Placement of Ultrasonic Transmitters and Receivers 4-16
4-14 Placement of Passive Infrared Sensors 4-17
5-1 Example of Mechanical Fence Sensor Installation 5-2
5-2 Typical Strain Sensor Cable Installation 5-3
5-3 Typical Taut Wire Installation 5-4
5-4 Typical Electric Field Sensor Detection Patterns 5-4
5-5 Typical Capacitance Sensor Configuration 5-5
5-6 Typical Ported Cable Detection Pattern 5-6
5-7 Typical Bistatic Microwave Beam Pattern 5-6
5-8 Typical Monostatic Microwave Sensor Detection Pattern 5-7
5-9 Typical Infrared Sensor Beam Patterns 5-7
5-10 Overlap of Fence-Mounted Sensor 5-11
5-11 Use of Strain-Sensitive Cable Around Corners 5-12
5-12 Overlap of Ported Cable Sensors 5-13
5-13 Microwave Dead Zone 5-14
5-14 Overlap of Microwave Zones 5-14
5-15 Microwave Layout Configurations 5-15
5-16 Stacked Microwave Configuration 5-15
5-17 Applications of Exterior Sensors at Perimeter Entry Points 5-16
5-18 Applications of Exterior Sensors Used for Intrusion Detection Around Perimeter Buildings 5-17
5-19 Complementary Exterior Sensors 5-19
6-1 Typical Point-to-Point IDS 6-2
6-2 Typical Multiplexed IDS 6-2
6-3 Typical IDS Alarm Annunciation System 6-2
6-4 Multiplexed DTM Configurations 6-6
6-5 Typical Redundant Computer Configuration 6-9
7-1 Magnetic Stripe and Wiegand-Effect Cards 7-2
7-2 Insertion and Swipe Card Readers 7-8
7-3 Biometric Device Error Rate Curves 7-8
7-4 Local Equipment Configurations 7-9
7-5 Centrally Controlled Entry Control System 7-10
7-6 Entry Control System Configured With Distributed Control 7-11
8-1 Typical CCTV Configuration 8-2
8-2 Typical CCTV Camera Components 8-2
8-3 CCTV Switcher Arrangements 8-7
8-4 Spectral Response 8-11
9-1 Examples of DC Supervision 9-3
10-1 Electronic Security System Electrical Power Block Diagram 10-2
11-1 Comparative Areas of Assessment by CCTV or Guard 11-2
11-2 Exterior IDS Configuration 11-4
11-3 Sequence of Design Development Events 11-5
C-1 Site Survey Support Request C-3
C-2 Preliminary Site Survey Information C-4

List of Tables

Table Title Page
4-1 Detection Range for Passive Ultrasonic Sensors 4-3
4-2 General Guidance for Application of IDS 4-11
4-3 Common Causes of Nuisance Alarms in Volumetric Sensors 4-15
5-1 Estimate of Probability of Detection by Exterior Sensors 5-9
5-2 Relative Susceptibility of Exterior Sensors to False Alarms 5-10
5-3 Exterior IDS Sensor Cost Comparison 5-10
7-1 Typical Verification Times of Entry Control Devices 7-6
7-2 Comparison of Coded Credential Cards 7-7
7-3 Security Level/Entry Control Matrix 7-12
8-1 Faceplate Dimensions: 1-inch, ⅔-inch, and ½-inch Image Formats 8-3
8-2 Typical Illumination Ranges of Common Sources 8-4
8-3 Scene Reflectance of Common Surfaces 8-4
8-4 Video Camera Light Range Requirements 8-4
8-5 Maximum Distance at Which a 7.5-inch Object May Be Recognized 8-9
8-6 Lens Selection Table: 1-inch Format 8-12
8-7 Lens Selection Table: ⅔-inch Format 8-13
8-8 Lens Selection Table: ½-inch Format 8-14

Table	Title	Page
8–9	Camera Placement Calculations: ⅔-inch Format	8–18
C–1	Recurrent Hours Matrix	C–13
C–2	Non-Recurrent Hours Matrix	C–14
C–3	Sample Estimated Survey Cost	C–14

CHAPTER 1

INTRODUCTION

1-1. Purpose

This manual establishes the requirements for electronic security systems. It describes ways to establish and implement criteria for design of electronic security systems for protection of Army facilities. It is intended to be used for the planning and design of electronic security systems by personnel who have the level of knowledge required for the design and specification of state-of-the-art electronic systems. This manual describes steps necessary to design a site-specific electronic security system with special attention to key interfaces. This design process requires the pre-existence of relevant support documentaion, such as site surveys, threat documentaion, generic design specifications, and cost estimating guides.

1-2. Scope

This manual is part of a series of security engineering manuals that describes the security engineering design process for facility design. Design guidance in this series of manuals spans the complete design cycle from initial programming to preparation of final plans and specifications. Each manual in the series is geared toward a specific security engineering user.

a. TM 5-853-1/AFMAN 32-1071, Volume 1. The project programmer will use this manual to define the protective system design criteria for a particular construction project and to develop a preconcept design of the protective system that can be used to estimate its cost.

b. TM 5-853-2/AFMAN 32-1071, Volume 2. The project design team will use this manual to bring the design to the concept (35 percent) level.

c. TM 5-853-3/AFMAN 32-1071, Volume 3. The various architect and engineering disciplines will use this manual to bring the design to completion. This manual provides design guidance related to resolving physical security issues as part of the building design process and includes information required to select and design protective meaures to resist a variety of threats.

d. TM 5-853-4. This manual will be used to design electronic security systems, including intrusion detection systems (IDS), closed circuit television (CCTV) alarm assessment systems, and electronic entry control systems (EECS).

1-3. References

Appendix A contains a list of references used in this manual.

1-4. Definition

An overall site security system is comprised of three major subelements: detection, delay, and response. The detection subsystem includes intrusion detection, assessment, and entry control. This manual addresses design of electronic security systems. An electronic security system is an integrated system that encompasses interior and exterior sensors, closed circuit television (CCTV) systems for assessment of alarm conditions, electronic entry control systems (EECS), data transmission media (DTM), and alarm reporting systems for monitoring, control, and display of various alarm and system information. Interior and exterior sensors and their associated communication and display subsystems are collectively called Intrusion Detection Systems (IDS). The systems are to be configured using proven, commercially available, off-the-shelf equipment, interfaced in some cases to existing systems.

1-5. Codes, Standards, and Regulations

Design of the electronic security system will incorporate all applicable industry and technical-society standards and codes and certifications and Army regulations that are in effect for the specific site at the time drawings and specifications are prepared. Symbols used to represent electronic security system equipment on design drawings will conform with the requirements of ASTM F 967.

1-6. Regulatory Requirements

Many Army regulations (AR) and Department of Defense (DOD) regulations specify protective measures, policies, and operations related to security. Appendix B contains a matrix indicating IDS-related requirements for various types of Army facilities. Although the regulations specify minimum requirements, it is possible that more stringent requirements will be necessary at specific sites. The designer will use the previously performed Site Survey to determine which regulations apply and to determine if any special circumstances require more stringent measures. The procedures used for this survey are shown in appendix C.

1-7. Use of Electronic Security Systems

Electronic security systems are to be fielded to provide early warning of attempted actions against Army assets by an intruder. Electronic security systems consist of hardware and software elements operating under control of trained security personnel. A system is configured to provide one or more layers of detection around the asset. Each layer is made up of a series of contiguous detection zones, designed to isolate that asset and control ingress and egress of authorized personnel and materials.

1-8. Interior Electronic Security Systems

Interior electronic security systems consist of sensors interfaced with electronic entry control devices, closed circuit television (CCTV), alarm reporting displays (both visual and audible), and security lighting. Assessment is accomplished by dispatching guards to the alarm point or by using CCTV for remote assessment. Alarm reporting devices and video monitors are located in the Security Center. Importance of the asset determines whether multiple or redundant Security Centers are required and, ultimately, the required sophistication of all elements in the interior electronic security system.

1-9. Exterior Electronic Security Systems

Exterior electronic security systems consist of sensors, interfaced with electronic entry control devices, CCTV, alarm reporting displays (visual, audible), and lighting. Assessment may be accomplished by dispatching guards to the alarm point or by use of CCTV for remote assessment; usually, CCTV assessment is deployed with exterior systems. The alarm reporting device and video monitors may share the same console in the Security Center used for interior systems, or they may stand alone. All exterior components must operate over a wide range of environmental conditions. The exterior system incorporates both alarmed perimeters and electronic entry control that are contiguous. An exterior system is normally effective only to the height of the fence along a width of 20 feet or less because of the limitations of sensor detection range.

1-10. Data Transmission

Digital and analog data are transmitted over a variety of media from local (field) interior and exterior locations to the Security Center for processing, display, and action by the console operator. Reliability and accuracy are important functional rquirements of the data transmission system.

1-11. State-of-the-Art

This manual describes subsystems and components that represent present state-of-the-art in hardware and technology and should provide adequate guidance in designing electronic security systems that use state-of-the-art components, without necessarily restricting the designer to components and systems described. New developments in electronic security system hardware and software will continue, necessitating that state-of-the-art developments be considered in future designs. As the state-of-the-art expands, improved technology will also be at the disposal of intruders. Intelligence information, transportaion, weapons, countersensors, and training, among other factors, will make future penetration attempts of sabotage and theft potentially more effective. Because electronic security is important to effective and efficient operations of security forces, familiarity with state-of-the-art hardware and design considerations is of utmost importance.

1-12. Reliability and Availability

Electronic security systems should be reliable and available for use by security forces. Although a long mean-time-between-failure (MTBF) for components and systems is required, systems have to be configured so that failure of a single element will not cause the system to become unavailable. Availability is affected adversely when the meat-time-to-repair (MTTR) of a component is too long, and by severe environmental conditions. Snow, fog, wind, or rain may become so severe as to render exterior IDS sensors temporarily unusable, thus placing reliance solely on the interior IDS. Proper in-depth system design of the system will reduce the impact of these environmental factors.

1-13. Expansion

Design of an electronic security system is based on general requirements tailored to a site-specific mission and physical profile. The design process generally begins with a top-down view of basic needs and classic configurations that are tailored to such site-specific characteristics as: terrain, geography of the site, climatic conditions, type of asset, and priorities. The data are used to determine hardware and software requirements, taking into account how much additional capacity should be factored into the design for future expansion.

1-14. Functional Equivalency

During the design process, specifications for the system, subsystems, and components must be prepared. The contract package will provide design configuration information and functional descriptions of hardware and software. The design configuration imposes fundamental physical features that will not be altered during construction and installation. When the designer has determined that commercial electronic security hardware is required, basic performance requirements are contained in specifications prepared with a variety of selectable parameters; those desired are determined during the design process and tailored by the designer for a site-specific system. Proposers responding to a request for proposal (RFP) will select from a variety of commercially available items for the project. Because many commercially available products have similar functions but different operating characteristics, key parameters must be accurately defined so that operating characteristics of the system will not be compromised. Specification parameters will be used to develop selection criteria to be used as the basis for evaluation of technical proposals.

1-15. Designer's Responsibility

The designer's responsibility is to determine and specify the types of hardware and software necessary to meet requirements, and how they are to be implemented.

1-16. Explanation of Abbreviations and Terms

Abbreviations and special terms used in this manual are explained in the Glossary.

CHAPTER 2

THREATS AND ASSETS

2-1. General

Each installation will have, by regulation, a classified threat statement, maintained current, normally on an annual basis. The threat statement is one of the factors used to define various intruder characteristics used against the installation's assets. The designer will be required to determine the appropriate types and quantities of electronic security components needed to protect the site or asset, based on the threat and asset to be protected. Refer to TM 5-583-1 for further guidance on determining the level and type of detection components required.

2-2. Threat Definition

a. A classified threat statement will contain information relative to numbers, skills, and equipment of intruders. Refer to TM 5-583-1 for a comprehensive discussion of aggressor threats and tactics.

b. Intruders may be classified as outsiders or insiders.

(1) Outsiders are not authorized to have access to an asset; their motivations are described in the classified document. The outsider may attempt to penetrate the system by forced entry or covert entry and by making use of insider compromise. Forced entry is a tactic of penetration in which the intruder does not try to avoid detection. Covert entry is an approach in which the intruder attempts to go around, over, or through the electronic security sytem without being detected. Covert entry may include the use of false credentials in an attempt to gain access to an asset. A well-conceived system will minimize successful use of covert entry and forced entry.

(2) Insiders may have a valid clearance and be authorized access to an asset on a need-to-know basis. In threatening to compromise an asset, they may act either covertly or overtly. Their motivations and reasons for acting against the government of the United States are part of the classified threat description. The designer protects against the insider by using such components as: contraband detectors at the entry control portal, tamper circuits, and internal closed circuit television (CCTV) for surveillance. The system must be designed so that it has no vulnerabilities or deficiencies that can be exploited without detection, whether the threat is from insiders or outsiders.

2-3. Asset Description

a. Every site has a complete description of all of its assets. Each asset has a relative importance to the national defense and is ranked in one of four levels (very high, high, medium, or low), as defined in AR 190-13. Minimum levels of protection, which are described in Army regulations, apply to each of the four categories (app B).

b. For purposes of IDS installation, all Army facilities will be designated as security levels A, B, C, or D, which are defined as follows:

(1) *Level A (Maximum Level Security).* This level of security is required for an area containing a security interest or defense asset, the compromise or loss of which would have an immediate effect on the defense potential or capability of the United States. Unauthorized access to the area could result in destruction or loss of control of the assets or disclosure of sensitive information. The total security effort for the area should provide the highest possible probability of detection, assessment, and prevention of unauthorized access to the protected items. The security system should detect any unauthorized penetration of the boundaries of the protected area because the mere presence of an intruder in the protected areas is unacceptable. Examples of areas that require level A security are nuclear and chemical weapons storage facilites and sensitive compartmented information facilities (SCIF).

(2) *Level B (Advanced Level Security).* This level of security is required for an area containing a security interest or defense asset, the compromise or loss of which would have a near-term effect on the defense potential or capability of the United States. The total security effort for the area should provide a high probability of detection, assessment, or prevention of unauthorized penetration, approach, destruction, or removal of the protected items. The security system should detect any unauthorized penetration of the boundaries of the protected area that results in introduction of contraband into the protected area or removal of or damage to sensitive items within the protected areas. Examples of areas which require level B security are designated limited areas and arms, ammunition, and explosives storage areas.

(3) *Level C (Intermediate Level Security).* This level of security is required for an area containing pilferable material or sensitive items that have a monetary value or an attraction for the intruder.

This level of security is also required foı equipment necessary for the continual functioning of the activity but not necessarily a part of the immediate or near-term mission or defense capability. The total security effort for the area should provide a reasonable probability of detection, assessment, or prevention of unauthorized penetration approach against destruction or removal of the protected items. The security system should detect any unauthorized penetration of the protected area that could result in removal of a protected item. Examples of areas which require level C security are ports, critical communications centers, power stations, and critical command posts.

(4) *Level D (Basic Level Security).* This level of security is required for an area established to protect pilferable items or for the principal purpose of providing administrative control or safety or a buffer for areas of a higher security category. Pilferable items within the area will require the same physical protection as level C. The security system should detect any unauthorized penetration of the protected area that could result in removal of a protected item. Examples of areas that require level D security are warehouses, motor pools, and designated controlled areas.

c. Any specific site may have a wide variety of assets, ranging from level A nuclear weapons to level D warehouses. The electronic security system required to protect them individually will vary in sophistication, but not in basic principles. TM 5–853–1 contains detailed procedures for determining the requirements for a site-specific electronic security system.

CHAPTER 3

SYSTEMS DESCRIPTIONS

Section I. CONFIGURATIONS

3–1. General

Electronic security systems consist of several major elements, with individul components and their associated interfaces. Major elements are IDS, CCTV, and EECS.

3–2. IDS Components

a. An IDS consists of the following major components: an alarm annunciation system, DTM, interior sensors, and exterior sensors. Refer to figure 3-1 for a typical configuration.

b. The alarm annunciation system is a modular, computer-based system that functions as the overall system coordinator, performing automated alarm functions, control of peripheral devices, operator interface, alarm reporting, and event logging.

(1) The operator interface displays alarms and data, accepts operator commands, and consists of a keyboard, color monitor, and/or map display.

(2) The alarm printer is dedicated to providing a permanent record of alarms and operator inputs associated with alarms and real-time control functions.

(3) The report printer is dedicated to generation of off-line reports.

(4) The hard disk is a high-density random access mass storage device, used to store system operations software and data.

(5) The floppy disk is a medium-density random access mass storage device, normally used for temporary storage of reports and data or for inital installation of software onto the hard disk.

(6) The magnetic tape system is a high-density mass storage device used to archive hard disk software and data for backup.

(7) The system real time clock with battery backup is used to synchronize system clocks at regular intervals, and will provide time data to CCTV and EECS.

(8) The map display is a pictorial representation of the site and sensors (zones) to provide a quick and convenient look at the system status.

(9) The CCTV interface transmits digital alarm data in a timely manner from the alarm annunciation system to the CCTV video switch, and receives alarm data from the video loss detector.

(10) The EECS interface receives digital alarm status data from the EECS central processor.

(11) The local (field) processor is a digital system located in an area protectd by interior or exterior sensors. The local processor monitors status of sensors and responds to transmissions from the alarm annunciation system.

c. The DTM is a data transmission link, such as wire lines, fiber optics, coaxial cable, or radio frequency transmission.

d. The interior intrusion detection sensors are devices used to detect unauthorized entry into specific areas or volumetric spaces within a building. The sensors generally perform one of three detection functions for a protected area: penetration of a boundary, motion within a boundary, or asset disturbance within a boundary.

(1) Boundary penetration sensors detect penetration through perimeter barriers, such as walls, ceilings, duct openings, doors, and windows and include:

(*a*) Vibration sensors.

(*b*) Heat sensors.

(*c*) Passive ultrasonic sensors.

(*d*) Door position sensors.

(*e*) Glass breakage sensors.

(*f*) Grid wire sensors.

(*g*) Photoelectric sensors.

(2) Volumetric motion sensors detect motion within a protected volume and include:

(*a*) Ultrasonic motion sensors.

(*b*) Microwave motion sensors.

(*c*) Infrared motion sensors.

(*d*) Video motion sensors.

(3) Point sensors detect an intruder coming close to, touching, or lifting an object and include:

(*a*) Capacitance sensors.

(*b*) Pressure mats.

(*c*) Pressure switches.

(4) Duress alarm devices are used to signal an emergency or a life threatening situation and may be either fixed or portable.

e. Exterior intrusion detection sensors detect an intruder crossing the boundary of an area being protected.

(1) Fence sensors detect attempts at climbing, cutting, or lifting fence fabric and posts and include:

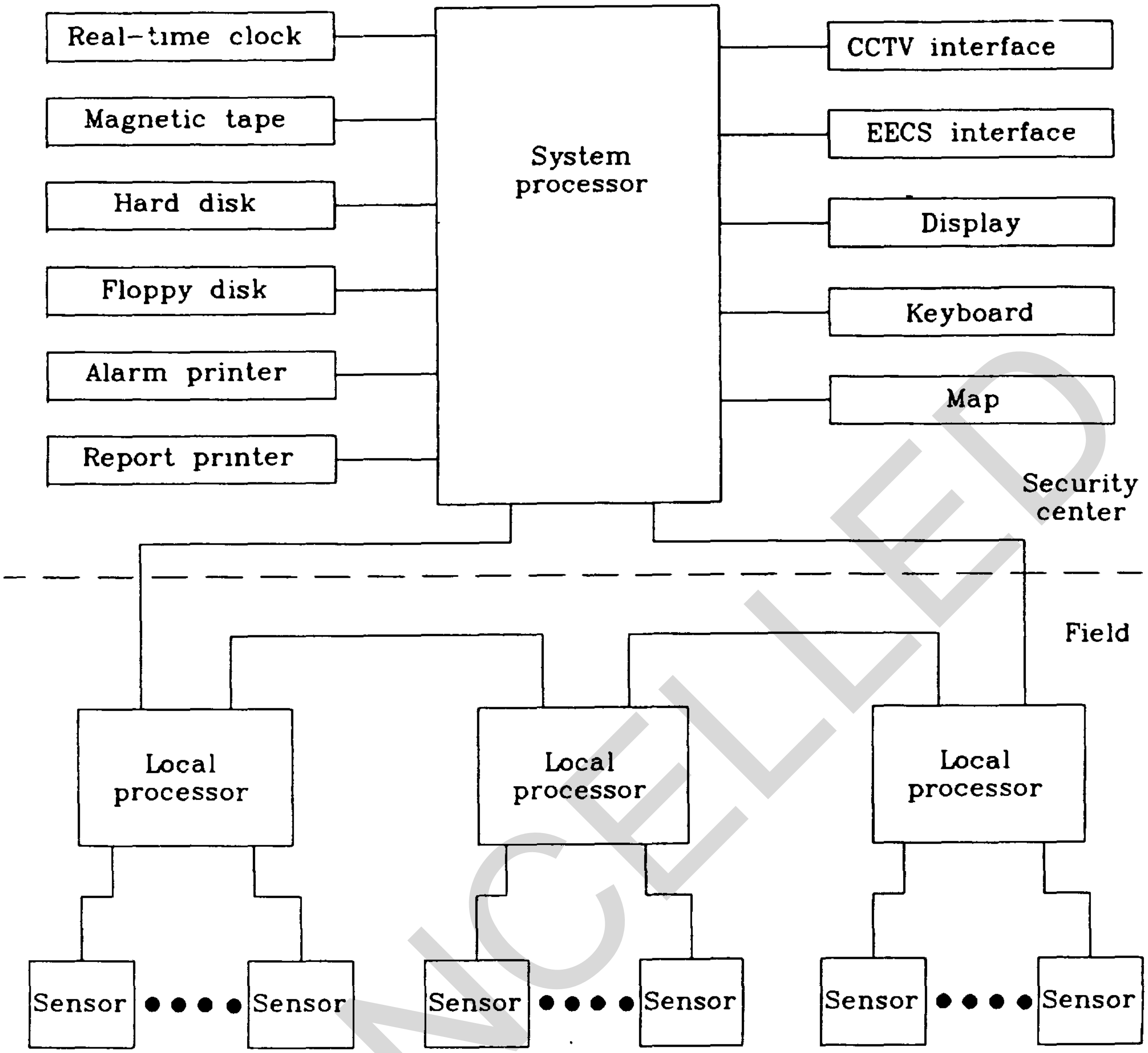


Figure 3-1 Typical IDS Configuration.

(*a*) Mechanical fence sensors.

(*b*) Electromechanical fence sensors.

(*c*) Strain sensitive cable sensors.

(*d*) Taut wire sensors.

(*e*) Electric field sensors.

(*f*) Capacitance proximity sensors.

(2) Buried line sensors, typically located between two fences that form an isolation zone, consist of detection cables buried in the ground.

(3) Line-of-sight sensors generate a beam of energy and detect a change in received energy caused by an intruder and include:

(*a*) Microwave sensors.

(*b*) Infrared sensors.

(4) Video motion sensors detect the presence of an intruder by comparing successive video images.

3-3. CCTV Components

a. The CCTV system consists of the following major components: video processing and display system, DTM, and cameras. Refer to figure 3-2 for a typical configuration.

b. The video processing and display system is a modular computer-based system that functions as the overall system coordinator performing automated video functions, control of peripheral de-

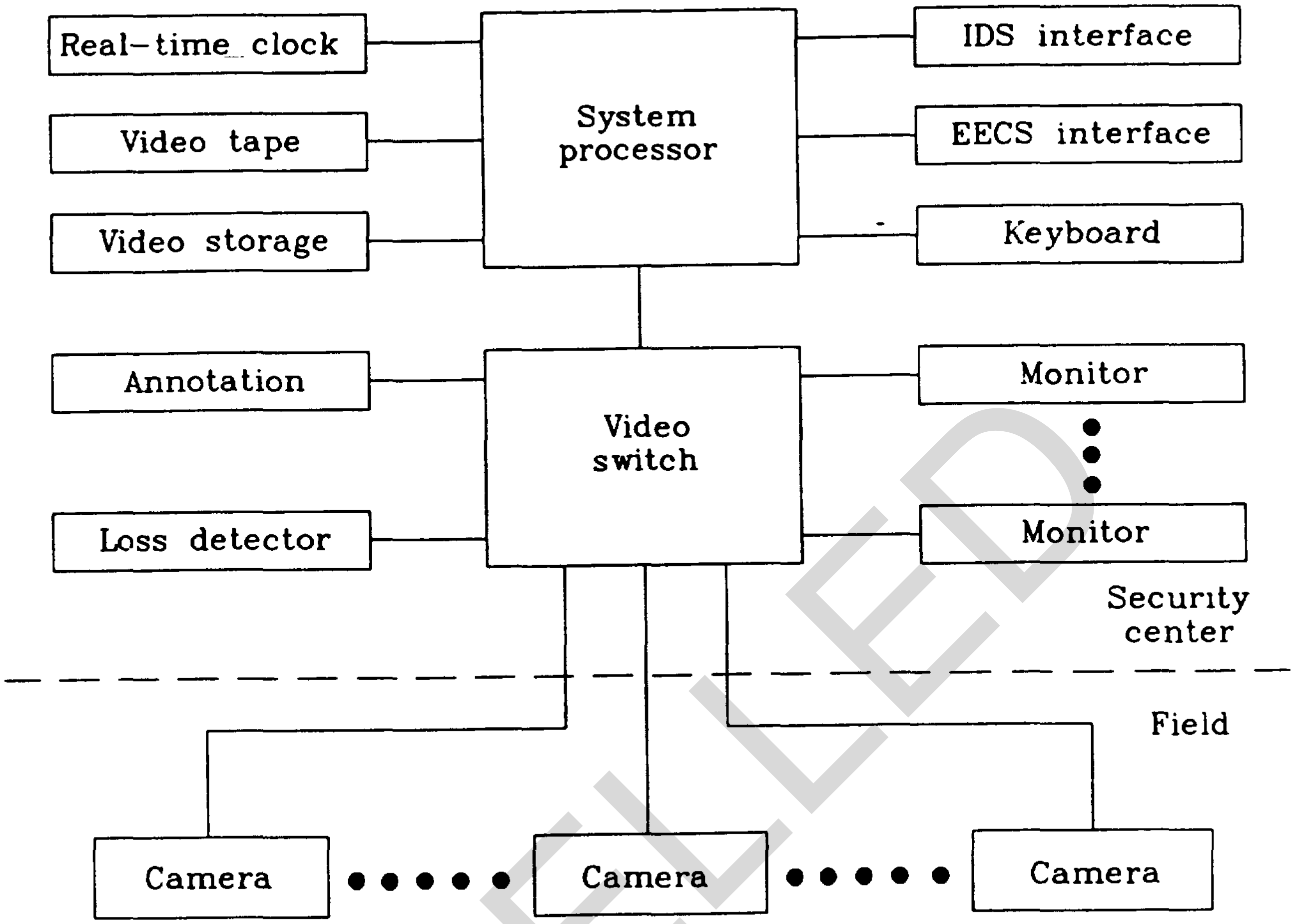


Figure 3-2. Typical CCTV System.

vices, operator interface, assessment and surveillance displays, and event logging.

(1) The operator's interface displays video images and camera identification and accepts operator commands. It consists of a keyboard, video monitors, and controls for pan, tilt, zoom cameras.

(2) The video switch is a modular system connecting the cameras to the monitors. The switch is controlled either by a digital processor or by the operator's keyboard.

(3) The video loss detector monitors each camera output for the presence of a video signal. The loss of signal is an alarm.

(4) Video monitors are black and white or color displays suitable for relay rack mounting. Multiple monitors may be used to assess alarms.

(5) Video storage devices use magnetic tape, hard disk, or solid state media. They store selected images for operator retrieval or archival use.

(6) Video annotation equipment provides camera identification and time data superimposed on the video image.

(7) The CCTV real-time clock is synchronized by the IDS clock and provides time data for video annotation.

(8) The IDS interface receives digital alarm data for the video switch for timely assessment and recording of alarms. The IDS interface transmits digital status data, for example, video loss.

(9) The EECS interface transmits each portal's location for coordination of video information with portal transactions and receives video switch data for camera/portal selection.

c. The DTM is a video and data transmission link such as wire lines, fiber optics, coaxial cable, or radio frequency transmission.

d. CCTV cameras are used to assess alarms and survey security areas. The cameras are either fixed field of view or pan, tilt, zoom variety for interior or exterior use.

(1) Five type of cameras use vacuum tube technology as the imaging media:

(*a*) Vidicon.

(*b*) Silicon diode.

(*c*) Silicon intensifier target.

(*d*) Intensified silicon intensifier target.

(*e*) Zinc selenide.

(2) Four types of cameras use solid state technology as the imaging media:

(*a*) Charge coupled.

(*b*) Charge priming.

(*c*) Metal oxide silicon.

(*d*) Charge-induced.

3-4. EECS Components

a. The electronic entry control system consists of the following major components: processing and display system, enrollment station, DTM, and entry control devices. Refer to figure 3-3 for a typical configuration.

b. The processing and display system is a modular computer-based system that functions as the overall system coordinator, performing automated entry, personnel accountability, alarm functions, control of peripheral devices, operator interfaces, alarm reporting, controlling locking devices, and event logging.

(1) The central processor uses the operating programs that govern ingress and egress transactions at portals to security areas. The programs may contain some or all the following functions:

(*a*) Logging.

(*b*) Time zoning.

(*c*) Area zoning.

(*d*) Occupant lists.

(2) The operator interface displays alarms and data, and accepts operator commands. It consists of a keyboard, video monitor, and manual control of locking devices.

(3) The alarm printer is dedicated to providing a permanent record of alarms and operator inputs associated with portal transaction, and real-time control functions.

(4) The report printer is dedicated to generation of off-line reports.

(5) The hard disk is a high-density random access mass storage device used to store system operations software and data.

(6) The floppy disk is a medium-density random access mass storage device that is normally used for temporary storage or initial installation of software onto the hard disk.

(7) The magnetic tape system is a high-density mass storage device used to archive hard disk software and data for backup.

(8) The real-time clock in the EECS is synchronized by the IDS, and is used for chronological time and control functions.

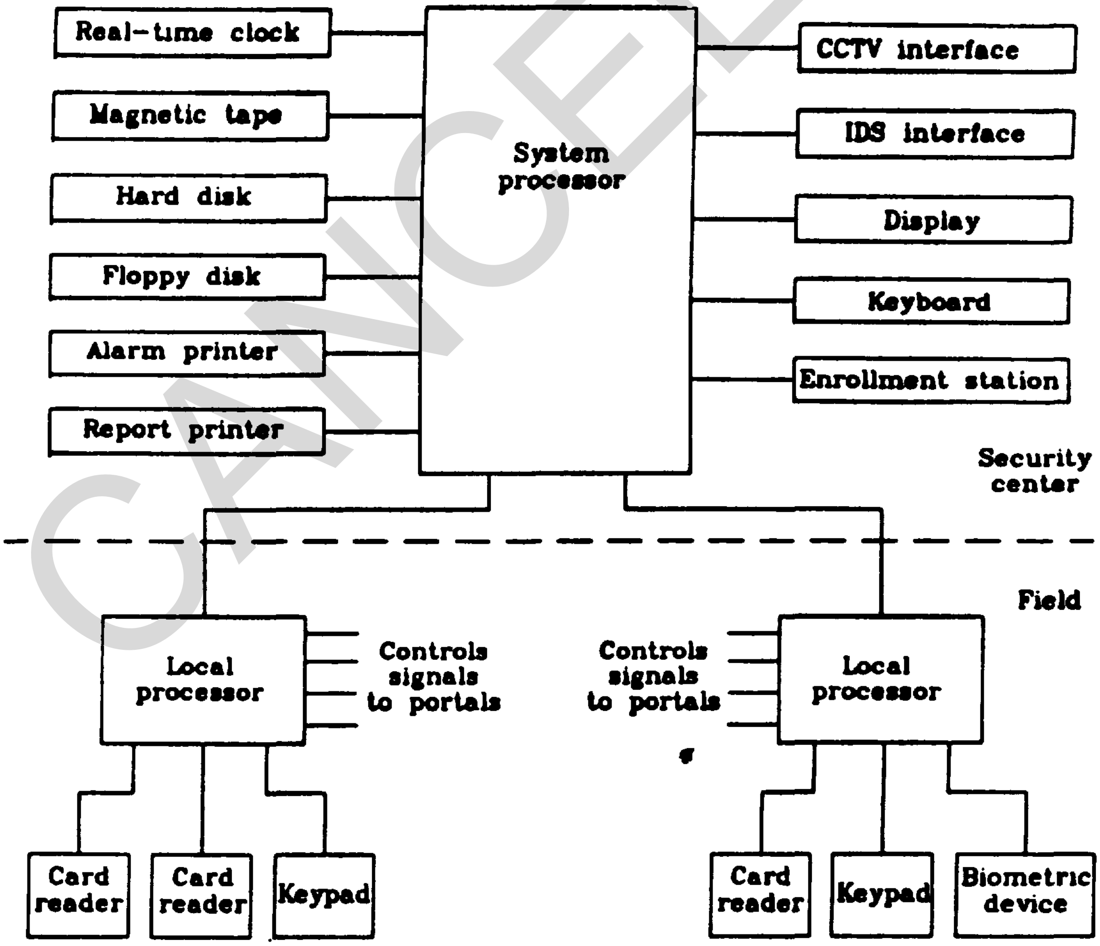


Figure 3-3. Typical EECS System.

(9) The CCTV interface transmits digital video switch data for camera/portal selection and receives portal location for coordination of video information.

(10) The IDS interface transmits digital alarm data and receives time update data.

(11) The local (field) processor is a digital system located near the portal. The local processor monitors the status of entry control devices and locking mechanisms and responds to signals from the processing and display system.

c. The enrollment station provides a means to enroll and disenroll personnel in the EECS. It consists of a dedicated keyboard and monitor and is usually located in an area other than the Security Center.

d. The DTM is a data transmission link, such as wire line, fiber optics, coaxial cable, or radio frequency transmission.

e. Automated entry control devices admit personnel using one or more of three basic techniques: coded devices, credential devices, or biometric devices. Enrollment stations are established so that personal data can be recorded and then used to authorize an individual into restricted areas. Enrollment stations are operated under supervision of the security manager, normally the Provost Marshal.

(1) Coded devices compare a manually entered code with a stored code.

(2) Credential devices compare machine readable code on a card or key with a stored code.

(3) Biometric devices measure one or more physical characteristics of an individual and compare this information with stored data.

Section II. STANDARD MILITARY SYSTEMS

3-5. Objective

The Department of Defense (DOD) objective is to acquire the most effective physical security system necessary for the protection of assets, including classified information and material. The DOD has developed and fielded standardized electronic security components and systems. Information on the components used in military systems must be obtained from the respective technical manuals. Before completing design of an electronic security system using military hardware or systems, the designer will verify availability of the equipment. If the equipment is not available, the using activity must obtain a waiver for use of equivalent commercially available equipment.

3-6. J-SIIDS

The Joint-Service Interior Intrusion Detection System (J-SIIDS) was developed primarily for protecting arms rooms. This limited system is used for interior IDS and consists of a control unit, DTM, balanced magnetic switch, capacitance proximity sensor, grid wire sensor, passive ultrasonic sensor, ultrasonic motion sensor, and a duress sensor. For further information see TM 5-6350-264-14-1.

3-7. BISS

The Air Force developed the Base Installation Security System (BISS) to protect special weapons and alert aircraft. This system is used for exterior systems and consists of a control unit, buried line sensors, fence sensors, bistatic microwave, and closed circuit television. For further information see SAFE-SIT-0001.

3-8. REMBASS

The Remotely Monitored Battlefield Sensor System (REMBASS) is an unattended ground sensor system that can detect the approach of wheeled vehicles, tracked vehicles, and personnel. This system is normally not used in fixed perimeter applications. It was developed for use on the battlefield but may be applicable to detection of intruders attempting to penetrate a controlled area. This system consists of a control unit, DTM, magnetic sensors, seismic sensors, and infrared sensors. For further information, see TM 11-6350-219-13.

3-9. FIEPSS

The Fixed Installation Exterior Perimeter Sensor System (FIEPSS) is the Army's exterior system adapted from selected BISS hardware. FIEPSS consists of a control unit, CCTV camera and switcher, CCTV poles, fence vibration sensor, and bistatic microwave sensor. The system must be monitored from a central control.

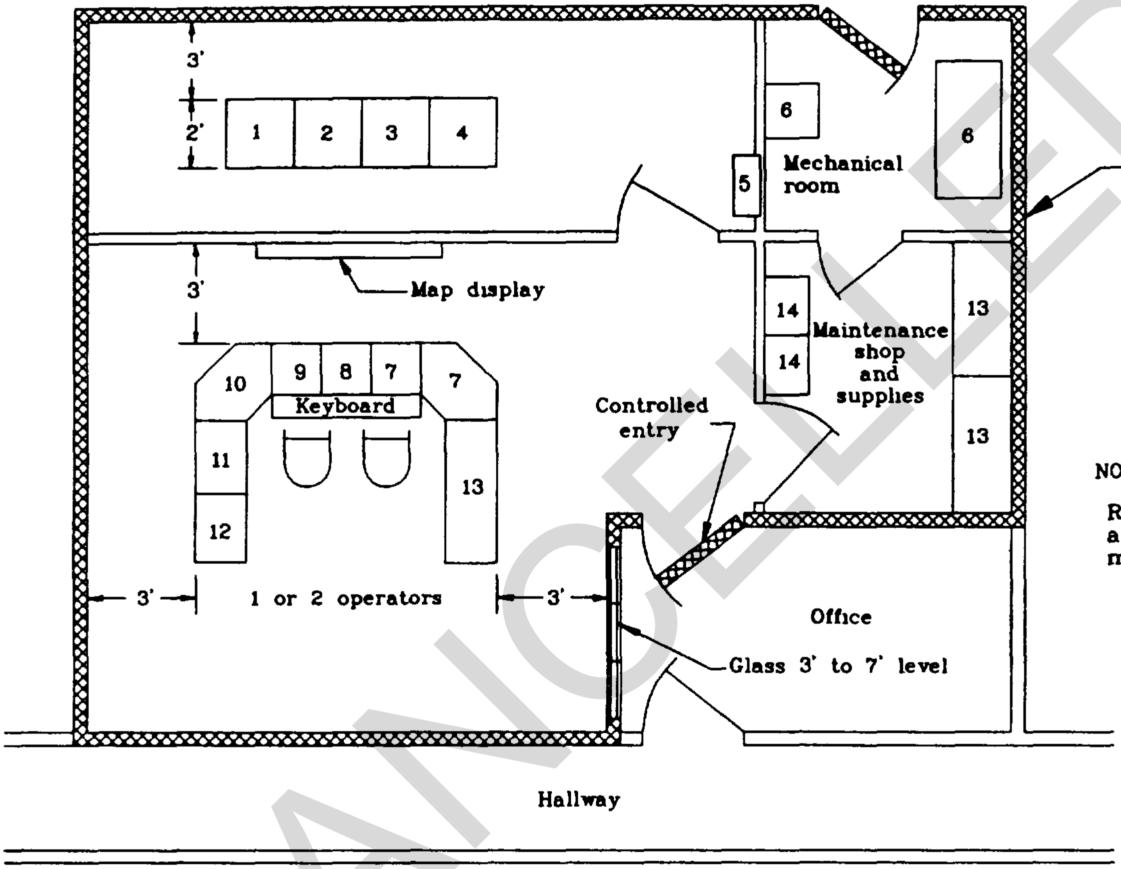
3-10. ICIDS

The Integrated Commercial Intrusion Detection System (ICIDS) is a tri-service program pursuing a nondevelopmental item acquisition using state-of-the-art technology. ICIDS consists of alarm annunciator, local (field) control units, interior and exterior sensors, CCTV, EECS, internal DTM, and uninterruptible power system. Research, development, testing, and engineering is programmed for completion in FY91.

Section III. SECURITY CENTER EQUIPMENT

3-11. Security Center Area

a. The Security Center is an area containing the alarm annunciation system, video processing and display system, EECS processing and display system, and other peripheral devices required. Environmental conditions will be maintained between 65 and 80 degrees Fahrenheit and between 40 and 60 percent relative humidity. It will be adequately soundproofed to attenuate noise from printers, equipment fans, and other noise-generating devices. Lockable space will be provided for storage of test equipment, spare parts, and other auxiliary equipment. Adequate space will be provided to allow supplier servicing of hardware. Typically, a clear zone of 3 feet is required at the front, rear, and sides of cabinets. Fire protection for the equipment will be provided as required by the installation's fire marshal. Figure 3-4 illustrates the type of layout required.



NOTE

Raised floor in all areas except mech room

1	Video switch and loss detector
2	Video processor, storage and annotation
3	IDS processor and storage
4	EEcs Processor and storage
5	Power panel
6	Back-up power
7	CCTV Monitors and keyboard
8	IDS display and keyboard
9	EECS display and keyboard
10	Map,intercom and telephone
11	Alarm printer
12	Report printer
13	Workspace
14	Storage

Figure 3-4. Typical Security Center Layout.

b. The operator responsible for monitoring and controlling this equipment has a multitude of functions to perform, including monitoring alarms from intrusion sensors, duress devices, electronic entry control equipment, and power equipment; assessment of alarms by means of CCTV and/or dispatching guards; placing sensors in access or secure mode; remote sensor testing and operational status verification; remote electronic entry control, as required; and assisting maintenance personnel by verifying operational status of repaired equipment. In addition to performing electronic security system functions, a typical operator may also be responsible for other security-related functions, such as radio communication, lock and key control, armory management, and emergency equipment management. Because of these responsibilities, the operator's console should be located in an area where outside disruptions or distractions are minimized. It is also vital that the equipment within this area be arranged in manner that enhances operator performance.

3-12. Console Consideration

a. A console is a set of standard or custom cabinets in which are mounted displays, controls, audio equipment, and other devices used to monitor and control remotely located (field) equipment. The primary factors to be considered in the design of a console are (1) what information should be displayed to the operator, (2) how the information should be displayed, and (3) how the operator interacts with the system. Because much of the electronic equipment installed in the Security Center is purchased as complete systems from commercial manufacturers, these questions have already been answered to the first order. Hence, the designer's primary task becomes one of integrating the different systems into a holistic arrangement that optimizes operator performance. The designer must select the optimum console configuration, the equipment to be installed in the console, and the arrangement of that equipment within the console. These factors are discussed in the following three subparagraphs. Additional information on console design can be found in MIL-STD 1472.

b. Although consoles can be configured to accommodate standing or seated operations, most Army Security Centers use an arrangement in which the operator is seated. A prime consideration is to assure that displays in the console can be easily viewed by the operator and that the controls are within easy reach. For small systems, the console equipment may require only two or three cabinets, in which case a straight line configuration may be suitable. For larger systems, requiring from three to five cabinets, a wraparound configuration is generally more suitable. Other factors to consider when selecting a console include (1) the number of persons who will require simultaneous access to the console; (2) requirements for visibility over the top of the console; (3) amount of panel space required, both above and below the writing surface; and (4) anthropometric data, that is, human measurements, such as functional reach and functional leg length when seated.

c. As part of the console selection and layout process, the designer must decide which equipment should be installed in the console and which should be installed elsewhere. This task can be accomplished by determining—

(1) What the operator must see (annunciator panels, monitors, indicators).

(2) What the operator must reach and manipulate (keyboards, push buttons, joysticks).

(3) What the operator must hear (alarms, telephones, speakers). To minimize console clutter and to simplify operator tasks, only equipment that is frequently used by the operator should be installed on the console. For example, with computer-based systems, an operator seldom interacts with the actual computer or disk storage devices. Likewise, an operator seldom interacts with the CCTV switcher or fiber optic drivers and receivers. Hence, this equipment should be located elsewhere. With small systems, it may be feasible to locate infrequently accessed equipment in the lower portion of the console, that is, below the writing surface. The lower portion of the console can also be equipped with shelves or drawers for storage of instruction manuals, logbooks, or other documents frequently used by an operator.

d. The working area of a console is the writing surface and the panel space above the writing surface. Because of the limited amount of space that is easily accessible by an operator, it is essential that equipment located in this area be organized in an efficient, coordinated manner. There are several methods that can be used to arrange displays and controls. One method is to arrange the equipment by function, that is, the displays and controls for each function, for example, CCTV assessment and surveillance, are grouped into one area of the console. Another method is to group the most frequently used controls in the area directly in front of the operator and infrequently used controls in the remaining areas. For applications using a predefined sequence of steps, a sequential organization may be used; that is, the controls are placed in sequential order so that the operator does not have to randomly skip over the console to find them. Of these methods, functional grouping is most often used in the layout of security-related consoles. A typical security console layout is shown in figure 3-5.

3-13. Room Layout

a. The physical layout or placement of the console and associated equipment depends on the physical configuration of the allocated area. For upgrades, the designer must usually adapt the equipment layout to an existing room (generally too small). For new facilities, the designer may have more flexibility in that he may be able to influence the size and shape of the allocated room. Major factors to consider in room layout are mobility, accessibility, lighting, and noise.

b. The room should have adequate space for the required number of operators. Operators should be able to move freely around equipment, around anyone performing a monitoring or control function, and around a maintenance person working on equipment. Whenever feasible, free floor space of at least 4 feet should be provided around each console. For equipment racks, the clearance from the rack to the nearest facing surface or obstacle should not be less than 3 feet.

c. All equipment should be positioned so that it is accessible for repair.

d. The interior lighting should be such that the operator's ability to view annunciator panels, indicators, and CCTV monitors is not degraded significantly. Light fixtures should be located so that reflections are not produced on monitors. Indirect lighting, for example, from recessed light fixtures, can be used to minimize reflections. Two separate lighting circuits should be provided, one for high-level lighting (50-100 footcandles) for maintenance purposes and one for low-level lighting (5-20 footcandles) for operational purposes. The low-level circuit should be provided with an adjustable control that permits an operator to adjust the light intensity for maximum contrast. Because of the tendency of fluorescent lights to flicker at low levels, incandescent lights should be used for the low-level circuit.

e. Audible noise within the room can reduce an operator's ability to concentrate as well as to communicate. The most bothersome sources of noise are ventilating fans, computer disk operations, and computer printer operations. Sound

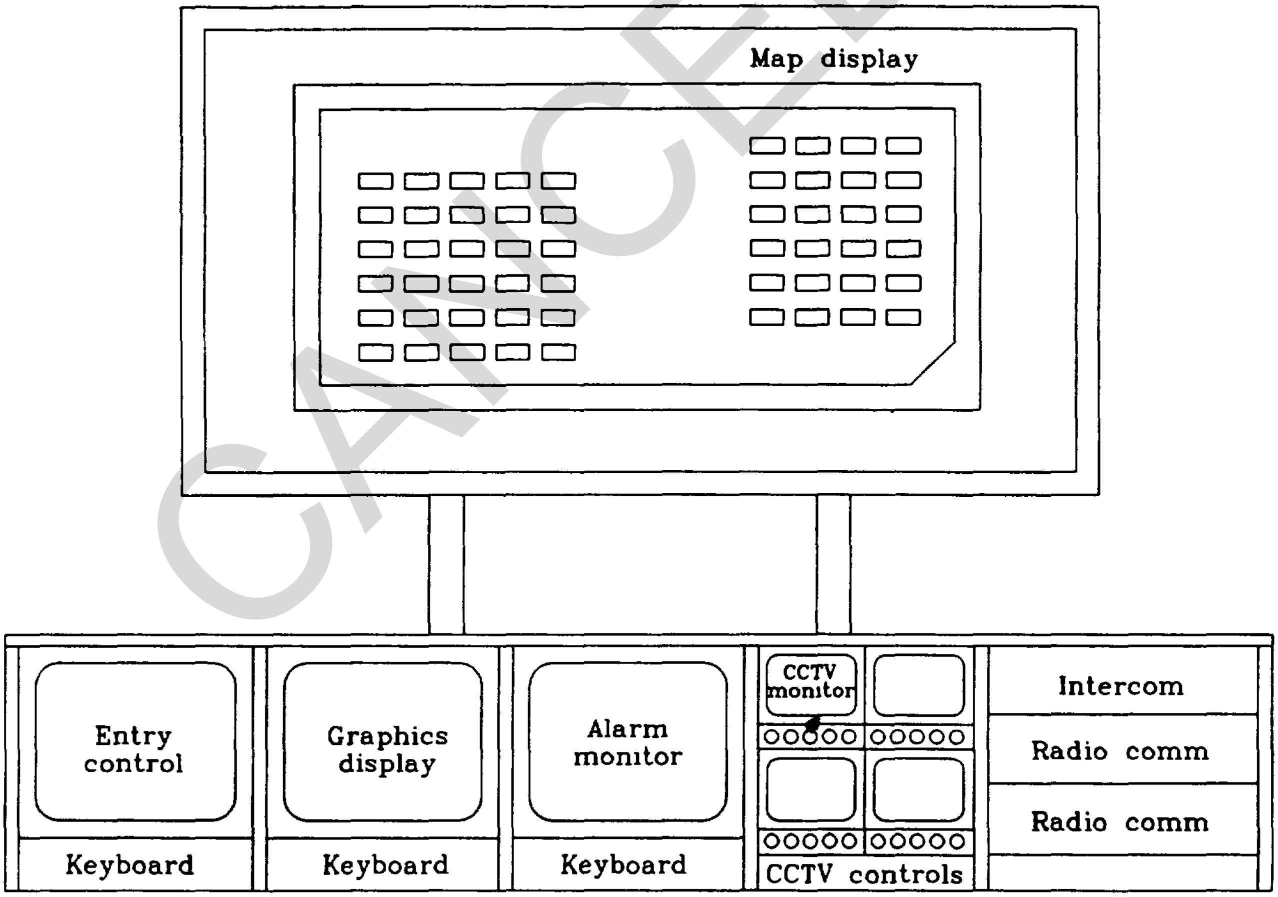


Figure 3-5 Typical Security Console Layout.

absorbing acoustical tiles can be placed on the walls and/or ceiling to reduce noise. Noisy equipment that need not be located in the console can be located in another room. Equipment racks can be fitted with sound absorbing material; however, this material may also reduce ventilation and result in overheating the equipment. The noise level for operational areas should not exceed 65 dB(A).

3-14. Other Considerations

a. Additional factors a designer should consider when planning the equipment layout in the Security Center are the operational environment, emergency power, and physical security.

b. A well-designed heating, ventilation, and air conditioning system for the Security Center is necessary to maintain operator alertness. It must have the capacity to handle the heat load generated by the equipment located in the console and other racks within the area (for additional information see MIL-HDBK-759).

c. All equipment located in the Security Center should be operable from the existing commercial ac power source. To protect against the loss of the commercial power source, an emergency power source should be provided. The emergency source should have enough capacity to power not only the electronic equipment but also the lighting, heating ventilating, and air conditioning equipment required to maintain operator alertness and efficiency. A minimum 4 hours backup capacity is required (for additional information see chap 10).

d. The Security Center is the single most vulnerable point of the electronic security systems, because of the large amount of equipment located there. As such, the Security Center should be provided with the same degree of security afforded to the most valuable asset in the facility. As a minimum, doors should be locked at all times and windows should be barred. Because the operator's console is usually manned 24 hours a day, interior IDS is not required for the area containing the console. However, the console should be equipped with a duress switch that signals an alarm in another location.

Section IV. GROUNDING, SHIELDING, AND TRANSIENT PROTECTION

3-15. Types of Interference

a. Digital logic and analog signal systems are susceptible to interference from two types of transients: functional and damaging upsets.

(1) Functional upsets are transients caused by inductive or capacitive coupling between data lines, control lines, and monitor lines that result in loss of data or improper control actions.

(2) Damaging upsets are transients caused by voltage surges, including indirect lightning strikes, that physically damage the equipment.

b. Power lines serving the system, nearby electrical and electromechanical devices, and lightning strikes are sources of transients.

c. Power line variations, due to transients from large starting loads or other disturbances, may cause temporary low voltage conditions to exist.

d. DTM links from the Security Center to the local processor must have surge protection circuits installed at each end and must also have triple electrode gas surge arresters within three feet of the building cable entrance.

e. Power circuits serving electronic security system equipment must be surge protected.

f. Control and sensor lines connected to electronic security system equipment must be surge protected.

3-16. Transient Protection Devices

Surge arresters provide low impedance paths to ground for surge voltage and lightning strikes that exceed threshold voltages ranging from 6.8 volts to 100,000 volts. A variety of different available devices can protect against lightning and other transients in power supplies, DTM lines, digital hardware, controllers, sensors, and cameras. Fuses and circuit breakers will be used for overcurrent protection. Transient protection devices will be used to protect control and monitor circuits, DTM circuits, and power inputs. Types of transient protection are—

a. Spark gaps.

b. Varistors.

c. Zener diodes.

d. Double anode zeners.

e. Crowbars.

f. Optical isolators.

g. Inductor capacitor resistor networks.

3-17. Grounding

The ideal grounding system is one which provides a zero impedance path for currents at all frequencies the system is expected to encounter. The most common type of grounding system consists of a grounding circuit that is terminated by copper clad steel rods driven into tbe ground. Use of building structural steel members in accordance with the NFPA 70 may be an acceptable means of grounding; however, in order to meet grounding resistance requirements, it may be necessary to combine several grounding techniques. Communications and instrumentation systems require a separate single point ground in addition to a power ground. Signal conductors that run parallel to primary power or lighting conductors will be avoided. Floating signal grounding systems, including those connected to the power "green wire" ground, are not acceptable because of probable lack of operating stability when used in instrumentation and other low signal applications. All enclosures will be tied to an equipment ground, which will be separate from communications and instrumentation grounds. Grounding will be in accordance with IEEE Standaıd 142. Additional grounding and power requirements exist for use in computer equipment areas such as the Security Center. These additional requirements, defined in FIPS-94, are to be incorporated in the Security Center design in addition to other stated requirements.

3-18. Shielding

Electronic circuits sensitive to EMI will be protected by electrical shielding. Shielding is used in telephone lines, twisted pairs, coaxial cables, and other circuits to reduce the strength of interfering electric or magnetic fields. Shielding will be grounded at one end only to preclude ground loops.

CHAPTER 4

INTERIOR INTRUSION DETECTION SENSORS

Section I. TYPES OF SENSORS

4–1. General

a. Interior intrusion detection sensors are devices used to detect unauthorized entry into specific areas or volumetric spaces within a building. These sensors are designed to operate indoors. They are usually not designed to be weatherproof nor rugged enough to survive an outdoor environment. Therefore, this type of sensor should not be used outdoors unless described by the manufacturer as suitable for outdoor use.

b. Interior intrusion detection sensors generally perform one of three detection functions: detection of an intruder penetrating the boundary of a protected area, detection of intruder motion within a protected area, and detection of an intruder touching or lifting an asset within a protected area. Hence, interior sensors are commonly classified as boundary penetration sensors, volumetric motion sensors, and point sensors. Although not intrusion detection sensors, duress switches are included in this discussion because they are usually wired to the same equipment that monitors IDS sensors.

4–2. Sensor Terminology

Before describing the various types of interior intrusion detection sensors, some common terminology used to describe sensor-related phenomena must be defined.

a. Alarm definitions. Alarms generated by an intrusion detection system can be classified as intrusion alarms, nuisance alarms, environmental alarms, and false alarms.

(1) Intrusion alarm. An intrusion alarm is the annunciation of an alarm resulting from the detection of a specified target; it represents an attempt to intrude into the protected area.

(2) Nuisance alarm. A nuisance alarm is the annunciation of an alarm resulting from the detection of a specified target, but it does not represent an attempt to intrude into the protected area.

(3) Environmental alarm. An evnironmental alarm is the annunciation of an alarm resulting from environmental conditions that exceed those specified.

(4) False alarm. A false alarm is the annunciation of an alarm resulting from no apparent cause.

b. False alarm rate. The number of false alarms per unit of time is termed the false alarm rate. This rate should not exceed one alarm per sensor per 5 days. A high rate reduces operator confidence in the system, which may lead to negligence in operator response. The false alarm rate usually may be reduced by lowering the sensitivity of a sensor; however, the probability of detection will also be lessened.

c. Standard intruder. For the purpose of this manual, a person with the characteristics of a 5th percentile US Army female will be considered a standard intruder. MIL–HDBK–759 defines this person as five feet tall, weighing 103 pounds, and this person is assumed to be wearing a long-sleeve shirt, slacks, and shoes, unless environmental conditions at the site require protective clothing.

d. Probability of detection. The probability of detection (PD) is a measure of a sensor's performance in detecting an intruder within its detection zone. It is a dimensionless number, normalized to a value between 0 and 1; for example a PD of 0.99 indicates that the sensor will detect an intruder 99 percent of the time. The PD of a sensor is profoundly affected by the method of installation, physical and environmental conditions of the facility, and differences in intruder penetration techniques. For example, the PD of a volumetric sensor can depend upon the direction, as well as velocity, of an intruder crossing its detection zone. Accordingly, conditions under which the PD of a sensor is specified must be carefully examined. A well-designed interior sensor should have a PD greater than 0.9, with a confidence level of 95 percent for the conditions specified. (Note: This equates to 49 successful detections out of 50 attempts or 96 out of 100.) Additional information on statistical reliability can be found in DODD3235.1.

e. Vulnerability to defeat. Another measure of sensor performance is its vulnerability to defeat. A sensor having a high PD and a low false alarm rate may not be a logical choice if it is easy to defeat. The use of tamper protection, signal line supervision, remote-test capability, and proper installation techniques will make sensors less vulnerable to defeat.

4-3. Boundary Penetration Sensors

Boundary penetration sensors are designed to detect penetration or attempted penetration through perimeter barriers, such as walls, ceilings, duct openings, doors, and windows. Penetration is detected by sensing physical phenomena generated by an attack on a barrier or wall surrounding the protected asset, or by detecting the actual intrusion. Structural vibration sensors, heat sensors, passive audio sensors, and passive ultrasonic sensors detect physical phenomena generated by an attempted penetration. Door position sensors, glass breakage sensors, foil tape, grid wire sensors, and photoelectric beams detect actual penetration.

a. *Structural vibration sensors.* Structural vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier. such as a wall or ceiling, by hammering, drilling, cutting, explosive detonation, or other forcible methods of entry.

(1) Two types of detection transducers are in use. One, a piezoelectric transducer, senses mechanical energy and converts it into electrical signals proportional in magnitude to the vibrations. The other, a mechanical switch, uses an inertial mass resting on a set of electrical contacts; vibration causes the mass to bounce, opening and closing the contacts. The intertial mass can be spring-loaded or unrestricted. A spring-loaded mass relies on the force of the spring to close contacts and can be mounted in any orientation. The unrestricted mass relies on its own weight to make contact and must always be mounted in a vertical position.

(2) To reduce false alarms from single accidental impacts on the barrier, most vibration sensors use a signal processor that has an adjustable pulse counting accumulator in conjunction with a manual sensitivity adjustment. The count circuit can be set to count a specific number of pulses of specific magnitude within a predefined time interval before an alarm is generated. However, the circuitry is usually designed to respond immediately to large pulses, such as those caused by an explosion. The sensitivity adjustment is used to compensate for the type of barrier and distance between transducers. Typically, several transducers can be connected together and monitored by one signal processor. Figure 4-1 shows an example of wall-mounted structual vibration sensors.

b. *Glass breakage sensors.* As the name implies, glass breakage sensors detect breaking of glass.

(1) The noise from breaking glass consists of vibration frequencies in both the audible and ultrasonic range. Glass breakage sensors use piezoelectric transducers similar to structural vibration sensors. However, the sensors are designed to respond to only higher frequencies, thus minimizing such false alarms as may be caused by banging on the glass.

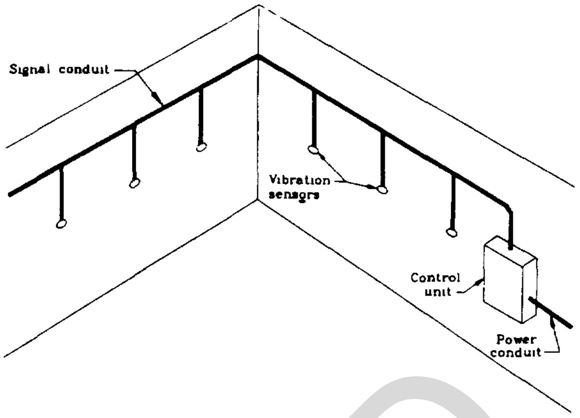


Figure 4-1 Wall-Mounted Structural Vibration Sensors.

(2) The signal processor initiates an alarm on the first high-frequency signal from the transducer. Pulse count circuitry is not used, because only one impact is usually enough to break the glass.

c. *Heat sensors.* Heat sensors are used to detect heat generated during penetration attempts made with a cutting torch or burn bar.

(1) These sensors are usually fixed-temperature devices that initiate an alarm when a preset temperature, typically 135 degrees Fahrenheit, is exceeded. There are two types, bimetallic and fusible link. Bimetallic sensors use materials that warp with increasing temperature and reset automatically as the temperature cools. The fusible link melts at the preset temperature and must be replaced, much like a blown fuse.

(2) Heat sensors can be used to detect thermal attacks on metal surfaces, such as vault doors or walls of a safe. To be effective, the temperature of the surface on which a sensor is mounted must reach the preset temperature before an alarm is activated. If the cutting technique used does not generate enough heat to raise the temperature of the surface to the preset temperature, an intruder could cut an access hole through the barrier without being detected.

d. *Passive audio sensors.* Passive audio sensors detect audible noises generated by forced entry into a protected area.

(1) The sensor detector consists of one or more microphones strategically located within the protected area to detect sounds in the audio frequency range. Microphones convert sounds into electrical signals that are sent to a signal processor.

(2) The signal processor has a manual sensitivity control with which the alarm threshold can be adjusted above normal audible background noise. Typical background noise can include outside sounds, such as those generated by trucks, airplanes, and trains, as well as inside noise, such as that generated by compressors, generators, and fans.

(3) Several signal processing techniques are used to minimize false alarms. Bandwidth of the processor can be adjsted to accept only frequencies within a predefined range, for example, between 1,500 and 6,000 Hz. Because most background noise occurs at frequencies below 1,500 Hz, this feature allows the alarm threshold level to be lowered, which increases sensitivity of the sensor. Adjustable pulse-counting circuits can be set to initiate an alarm only after counting a selected number of noise pulses within a specific time period. This feature reduces false alarms from noises that exist only briefly, such as thunder. Another technique for reducing false alarms is to use cancellation microphones, which can be installed outside the protected area of near known noise sources. Signals from cancellation microphones are used to cancel corresponding signalks received by the detection microphones.

(4) Although described signal processing techniques can reduce the number of false alarms caused by undesirable noise sources, they also reduce the probability of detection. For example, signal processors with pulse-counting circuitry may not respond to noise generated by extremely slow movement. If cancellation microphones are used, a highly skilled intuder can synchronize his or her movements with loud outside noises.

(5) An advantage of using passive audio sensors is that microphones can provide audio assessment of the protected area. When an alarm occurs, the signal transmission line can be connected to the microphones, so that the operator in the Security Center can listen to noise that caused the alarm. This listen-in capability is present only when the sensor is in the "secure" mode and in an alarm state. When the sensor is reset or placed in the "access" mode, an operator no longer can listen-in.

e. Passive ultrasonic sensors. These detect acoustical energy in the ultrasonic frequency range, typically between 20 and 30 kHz. They are used to detect attempted penetration through rigid barriers, such as metal or masonry walls, ceilings, and floors. They also detect penetration through windows and vents covered by metal grills, shutters, or bars, if these openings are properly sealed against outside sounds.

(1) The detection transducer is a piezoelectric crystal that produces electrical signals proportional to the magnitude of the vibrations. A single transducer provides coverage of an area approximately 15 by 20 feet in a room with an 8-foot to 12-foot ceiling. A typical detection pattern is shown in figure 4-2. Up to 10 or more transducers can be connected to a signal processor. As with vibration sensors, the signal processor for a passive ultrasonic sensor has manual sensitivity adjustment and an adjustable pulse-counting accumulator.

(2) Passive ultrasonic sensors detect ultrasonic energy that results from breaking glass, snipping of bolt cutters on metal barriers, hissing of an acetylene torch, and shattering of brittle materials, such as concrete or cinderblock. However, the sensors will not reliably detect drilling through most materials nor attacks against soft material such as wall board. Their effective detection range depends largely on barrier material, method of attempted penetration, and sensitivity adjustment of the sensor. Examples of maximum detection distances for a typical sensor for different types of attempted penetration are shown in table 4-1.

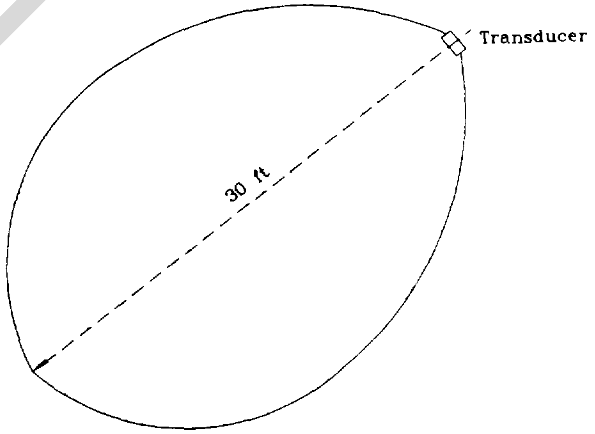
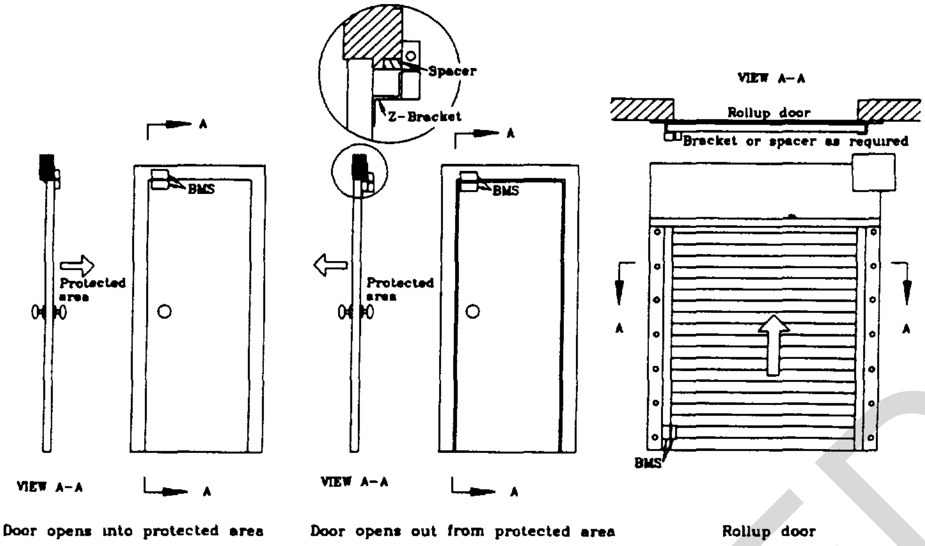


Figure 4-2. Typical Passive Ultrasonic Sensor Detection Pattern

Table 4-1 Detection Range For Passive Ultrasonic Sensors

Type of Penetration	*Distance*
Cut ¼-inch thick expanded metal with bolt cutter	55 ft
Cut ⅝-inch reinforcing bar with bolt cutters	45 ft
Use acetylene cutting torch	39 ft
Cut wood with circular saw	30 ft
Cut ⅝-inch reinforcing bar with hacksaw	19 ft
Drill through brick	15 ft
Drill through ⅛-inch steel plate	6 ft
Cut ⅛-inch steel plate with hacksaw	4 ft
Drill through cinderblock	3 ft



Door opens into protected area   Door opens out from protected area   Rollup door

Figure 4-3. BMS Mounting Configurations

f. Door position sensors. Mechanical contact switches and magnetic switches are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry.

(1) Mechanical contact switches are either push button or lever type. Push button switches are usually mounted on the hinge side of door frames, while lever switches are installed along the top of door frames. Either kind may be used as a vault door switch, where movement of the locking bolt mechanism, rather than movement of the door, actuates the switch.

(2) Two types of magnetic switches are available, a simple magnetic contact switch and a balanced magnetic switch (BMS). With these sensors, the switch mechanism is mounted on the door frame and the actuating magnet on the door. The simple contact switch uses a two-position reed switch, which is held in either an open or closed position by the magnet on the closed door. Moving the magnet by opening the door causes the switch to move to the other position, generating an alarm. Typically, the BMS has a three-position reed switch and an additional magnet, called the bias magnet, located adjacent to the switch. When the door is closed, the reed switch is held in the balanced or center position by interacting magnetic fields. If the door is opened or an external magnet is brought near the sensor in an attempt to defeat it, the switch becomes unbalanced and generates an alarm.

(3) Because of their resistance to being defeated, only balanced magnetic switches should be used in Army facilities. They must be mounted so that the magnet receives maximum movement when the door or window is opened. Figure 4-3 shows several configurations for mounting balanced magnetic switches on doors.

g. Foil tape. This type of sensor consists of a conducting tape that is attached to the surface of a barrier, such as a wall or glass window. The tape is usually arranged in a loop, through which an electrical current flows. If the tape is broken, an open circuit is created, generating an alarm. The tape is attached to the window with a special adhesive that must be able to withstand aging, moisture, sunlight, and temperature extremes. When used on windows, foil tape is very visible. It may act as a deterrent or, conversely, it may define the area where a hole can be successfully cut in the glass without breaking the tape. Foil tape is seldom used for the protection of Army facilities because it can be so easily defeated.

h. Grid wire sensors. This type of sensor consists of a continuous electrical wire arranged in a grid pattern. As with foil tape, an electrical current is maintained in the wire. When the wire is broken, an alarm is generated. This sensor is used to detect forced entry through walls, floors, ceilings, doors, windows, and other barriers.

(1) Typically, an enamel-coated, number 24 or 26 AWG solid copper wire is used to form the grid, the maximum size of which is determined by spacing between the wires, resistance of the wire, and electrical characteristics of the source providing the current.

(2) The grid wire can be installed directly on the barrier, or in a grill or screen that is mounted on the barrier or over an opening that requires protection. The wire can be stapled directly to barriers made of wood or wallboard. Wood panels should be installed over the grid to protect if from day-to-day abuse and to conceal it. When used on

cinder, concrete, and masonry surfaces, these surfaces must first be covered with plywood or other material to which the wire can be stapled. An alternative method is to staple the wire grid to the back side of a panel and install the panel over the surface.

(3) Grid wire sensors are virtually nuisance alarm free, except in some instances under very humid conditions, where it is possible to cause low resistance paths to occur between adjacent conductors or between adjacent conductors and ground.

i. Photoelectric beam sensors. These transmit a beam across the area to be protected. When the beam is interrupted, an alarm is generated.

(1) The photoelectric beam sensor consists of a light transmitter and a receiver. The transmitter is located on one side of the entrance or area being protected and the receiver is located on the opposite side, aligned to receive light energy from the transmitter. An alarm is generated whenever the beam is interrupted. Early sensors used an incandescent light source in the transmitter; the light was passed through a red filter to reduce its visibility. Contemporary sensors use an infrared light beam generated by a gallium arsenide light-emitting diode (LED).

(2) To minimize the possibility of an intruder defeating the sensor with another light source, the transmitter light source can be modulated by turning it on and off at a specific frequency. The receiver accepts only light at the correct modulation frequency and is designed so that the photocell acceptance angle is narrow, requiring a substitute light source to be placed at an exact angle to be successful.

(3) Mirrors can be used to reduce the number of sensors required; they can also be used to cover difficult areas, such as corners. However, use of mirrors reduces the effective range of sensors because not all of the beam is reflected by the mirror; a portion is refracted and scattered.

(4) Smoke or dust within the protected area will diminish the intensity of the sensor beam enough to cause false alarms. Other potential sources of false alarms are falling objects, birds, and animals. Accumulation of dirt on sensor lenses and mirrors can also cause problems. Alignment, especially when mirrors are used, is critical. To prevent misalignment, sensors and mirrors should be securely mounted on a surface that does not vibrate.

(5) Photoelectric sensors can be used to protect entrances and to form a square or rectangular barrier around an open or enclosed area. To reduce the potential vulnerability caused by an intruder bypassing the beam, at least two beams should be used, one located approximately 12 inches above the floor, the other 30 inches above the floor. Several photoelectric beam sensor configurations are illustrated in figure 4-4.

4-4. Volumetric Motion Sensors

Volumetric motion sensors are designed to detect intruder motion within the interior of a protected volume. Volumetric sensors may be active or passive. Active sensors, such as ultrasonic and microwave, fill the volume to be protected with an energy pattern and recognize a disturbance in the pattern when anything moves within the detection zone. Whereas active sensors generate their own

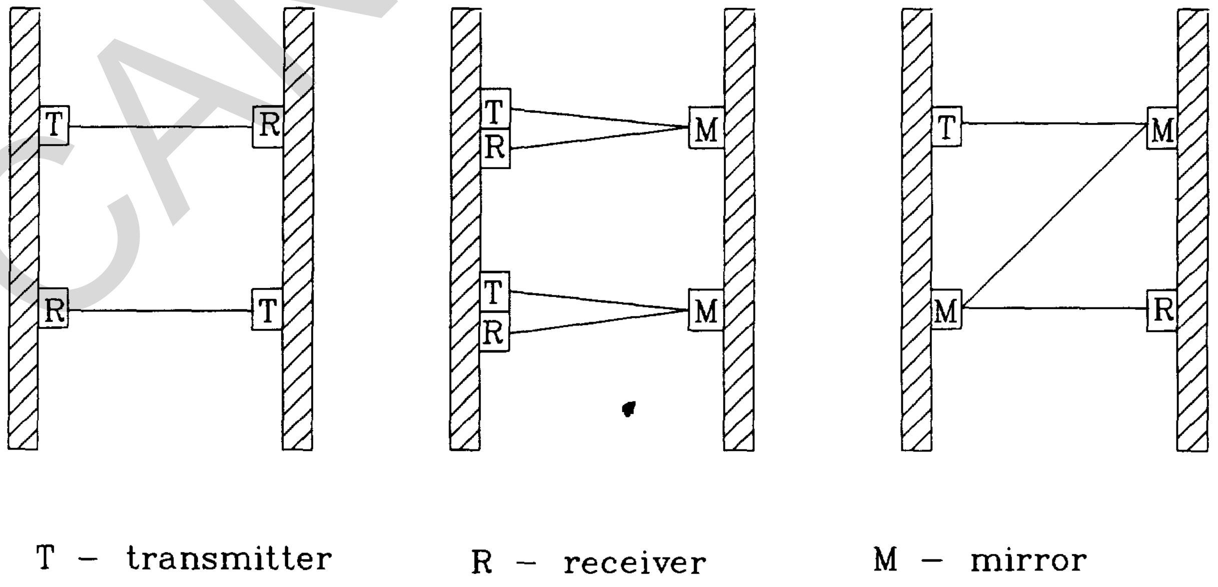


Figure 4-4. Photoelectric Beam Sensor Configurations.

energy pattern to detect an intruder, passive sensors, such as infrared, detect energy generated by an intruder. Some sensors, known as "dual-technology" sensors, use a combination of two different technologies, usually one active and one passive, within the same unit. If CCTV assessment or surveillance cameras are installed, video motion sensors can be used to detect intruder movement within the area.

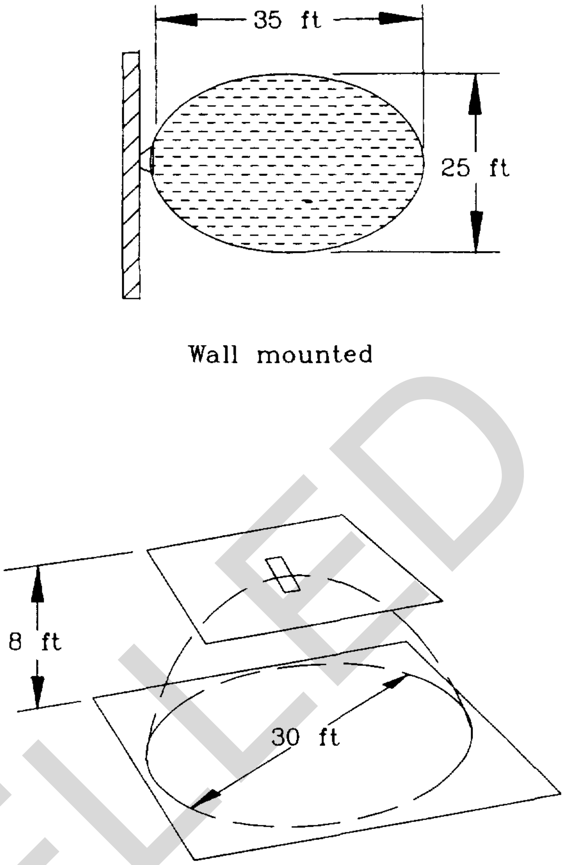
a. Ultrasonic motion sensors. Ultrasonic motion sensors generate high-frequency sound waves and respond to changes in these waves caused by intruder movement within the protected area.

(1) Most ultrasonic motion sensors in use today use the principle of Doppler frequency shift as their basis of operation. The apparent change in frequency is caused by the compression and expansion of the sound waves produced by the relative motion between sound source and receiver.

(2) An ultrasonic motion sensor consists of a transmitter, receiver, and signal processor. The transmitter generates an acoustical energy pattern, typically at a specific frequency in the range of 19–40 kHz, above the frequencies humans can hear. Energy reflected from walls, ceiling, floor, and stationary objects within the energy pattern is sensed by the receiver and analyzed by the signal processor. As long as reflected energy is at the same frequency as transmitted energy, there is no alarm. However, an intruder moving within the energy pattern produces a Doppler frequency shift in the reflected signal that caused an alarm. The energy generated by an ultrasonic sensor is completely confined within the area in which it is operating. It does not penetrate walls or windows.

(3) Piezoelectric and magnetostrictive transducers are used in transmitters and receivers to convert electrical energy into acoustical energy and vice versa. The shape of the energy pattern produced by the transmitter depends on the shape and dimensions of the transducer. A disc-shaped piezoelectric transducer produces a conical beam pattern, where a ring-shaped transducer produces a circular pattern. Typical ultrasonic beam patterns are shown in figure 4-5.

(4) There are two basic sensor configurations in use: the transceiver (or monostatic) and the multihead (or bistatic). The transceiver is a single unit that houses both transmitter and receiver. The signal processor and power supply can be mounted in the transceiver enclosure known as a control unit. With a multihead configuration, transmitter and receiver are mounted in separate enclosures and installed 20 to 30 feet apart. The signal processor and power supply are usually mounted in a separate enclosure, the control unit. A single control unit can typically handle several pairs of heads or several transceivers.



Wall mounted

Ceiling mounted

Figure 4-5. Typical Ultrasonic Motion Sensor Beam Patterns.

(5) A major difference between various ultrasonic motion sensors is the manner in which the Doppler signal is processed. As with many sensors, major emphasis is on reduction of false alarms. One technique is to use a bandwidth filter to remove all frequencies above and below the operating frequency of the sensor. Because typical intruder motion produces frequency shifts between 30 and 800 Hz, the width of the bandpass filter is approximately 2,000 Hz. Another technique uses automatic gain control circuitry to adjust the alarm threshold automatically and thus compensate for fluctuating background noise in the ultrasonic range. A third technique used is to respond only to a net change in Doppler frequency, where an intuder moving towards or away from the sensor will produce a net positive or negative frequency shift, depending on the direction of motion. Curtains and drapes, when exposed to air drafts, will move in a slow oscillatory motion that produces both positive and negative frequency shifts that result in no net change. Finally, some

sensors use time delay circuitry that requires the Doppler signal be present for several seconds before an alarm is generated. This technique eliminates false alarms from short-duration noises such as telephone rings.

b. Microwave motion sensors. These sensors are similar to ultrasonic motion sensors, except that high-frequency electromagnetic energy, rather than acoustical energy, is used to detect intruder motion within the protected area.

(1) Interior microwave motion sensors are typically monostatic, that is, transmitter and receiver are housed in the same enclosure (transceiver). The transmitter and receiver may each be provided with a separate antenna or may share a common antenna. The high frequency signals produced by the transmitter are usually generated by a solid-state device, such as a gallium arsenide field-effect transistor. The power generated is usually less than 10 milliwatts, but is sufficient to transmit the signal for distances up to approximately 100 feet. The shape of the transmitted beam is a function of the antenna configuration. The range of the transmitted beam can be controlled with a range adjustment. A wide variety of detection patterns can be generated, several of which are shown in figure 4-6.

(2) The signal processing techniques used in microwave motion sensors are similar to those used in ultrasonic motion sensors. Frequency of the transmitted signal is compared with frequency of the signal reflected back from objects in the protected area. If there is no movement within the area, the transmitted and received frequencies will be equal and no alarm will be generated. Movement in the area will generate a Doppler frequency shift in the reflected signal and will produce an alarm if the signal satisfies the sensor's alarm criteria. The Doppler shift for a human intuder is typically between 20 and 120 Hz.

(3) Unlike ultrasonic energy, microwave energy can pass through glass doors and windows as well as lightweight walls or partitions constructed of plywood, plastic, or fiber board. As a result, false alarms are possible because of reflection of the microwave signals from movement of people or vehicles outside the protected area. The designer can sometimes take advantage of this when the protected area is large and contains a number of partitions, but this is not normally done.

(4) Federal Communication Commission (FCC) regulations cover the design, manufacture, installation, and maintenance of microwave motion sensors. Five frequency bands have been assigned: 915 MHz, 2,450 MHz, 5,800 MHz, 10,525 MHz, and 22,125 MHz. Most commercial sensors operate in the 10,525 MHz frequency range. FCC regulations governing unlicensed use of field disturbance sensors can be found in FCC Part 15.

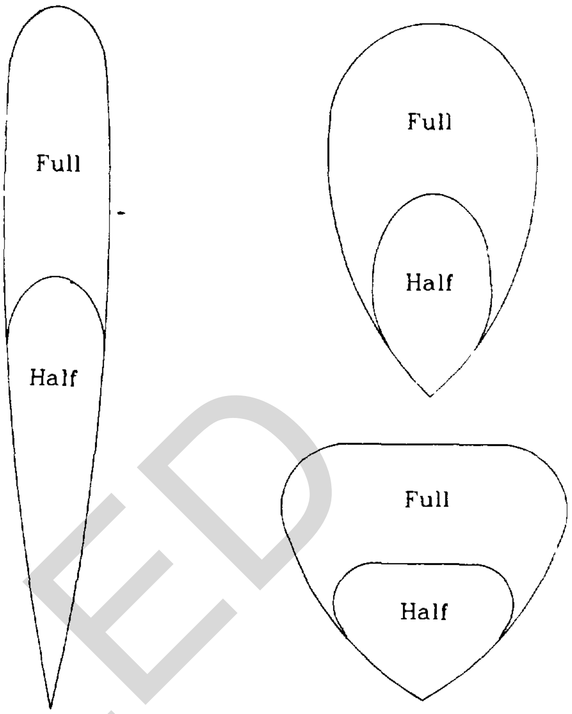


Figure 4-6 Typical Detection Patterns for Microwave Motion Sensors.

c. Passive infrared motion sensors. Passive infrared motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.

(1) All objects with temperatures above absolute zero radiate thermal energy. The wavelengths of the infrared energy spectrum lie between 1 and 1,000 microns. Because the human body radiates thermal energy of between 7 and 14 microns, passive infrared (PIR) motion sensors are typically designed to operate in the far infrared wavelength range of 4 to 20 microns.

(2) The infrared energy must be focused onto a sensing element, somewhat as a camera lens focuses light onto a film. Two techniques are commonly used. One technique uses reflective focusing; that is, parabolic mirrors focus the energy; the other uses an optical lens. Of the various types of optical lenses, Fresnal lenses are preferred because they can achieve short focal lengths with minimal thickness. Because infrared energy is severely attenuated by glass, lenses are usually fabricated of plastic.

(3) The detection pattern of the sensor is determined by arrangement of lenses or reflectors. The pattern is not continuous but consists of a number of rays or fingers, one for each mirror or lens segment. Numerous detection patterns are available, several of which are shown in figure 4-7. The PIR is not provided with a range adjustment, but range can be adjusted somewhat by adjusting the position of the sensor; therefore careful selection of the appropriate detection pattern is critical to proper sensor performance.

(4) Almost all manufacturers today use a pyroelectric material as the thermal sensing element. This material produces a change in electric charge when exposed to changes in temperature. To minimize false alarms caused by changes in ambient temperature, most manufacturers use a dual-element sensor: the sensing element is split into halves, one of which produces a positive voltage pulse and the other a negative pulse when a change in temperature is detected. The pulses cancel each other, thus eliminating the effects of ambient temperature changes. However, an intruder entering one of the detection fingers produces an imbalance between the two halves, resulting in an alarm condition. Quad-element sensors that combine and compare two dual-element sensors are also in use. Pulse-count activation is another technique used to reduce false alarms. With this technique, a predefined number of pulses within a specific interval of time must be produced before an alarm is generated.

d. Dual-technology sensors. To minimize generation of alarms caused by sources other than intruders, these sensors combine two different technologies in one unit. Ideally, this is achieved by combining two sensors that, individually, have a high probability of detection and do not respond to common sources of false alarms.

(1) Available dual-technology sensors combine either an active ultrasonic or microwave sensor with a passive infrared sensor. The alarms from each sensor are logically combined in an "AND" configuration; that is, nearly simultaneous alarms from both active and passive sensors are needed to produce a valid alarm.

(2) Although combined technology sensors have a lower false alarm rate than sensors used individually, probability of detection is also reduced. For example, if each individual sensor has a PD of 0.95, PD of the combined sensors is the product of individual probabilities, 0.9. Also, ultrasonic and microwave motion sensors have the highest probability of detecting movement directly toward or away from the sensor, whereas passive infrared motion sensors have the highest probability of detecting movement across the detection pattern. Therefore, the PD of sensors combined in a single unit is less than that obtainable if the individual sensors are mounted perpendicular to each other with overlapping detection patterns. However, because of the lower false alarm rate,

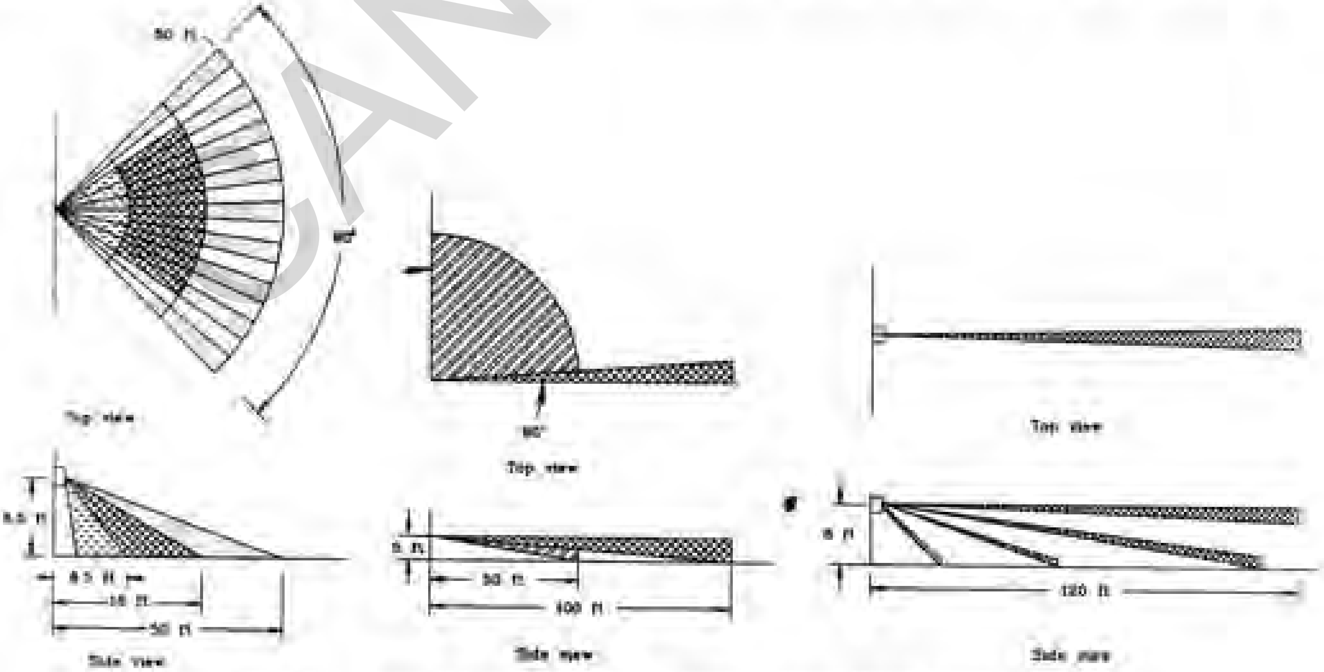


Figure 4-7. Typical Detection Patterns for a Passive Infrared Motion Detector.

the reduced PD can be somewhat compensated for by increasing the sensitivity or detection criteria of each individual sensor.

e. Video motion sensors. A video motion sensor generates an alarm whenever an intruder enters a selected portion of a CCTV camera's field of view. The sensor processes and compares successive images from the camera and generates an alarm if differences between the images satisfy predefined criteria.

(1) There are two categories of video motion detectors: analog and digital. Analog detectors generate an alarm in response to changes in picture contrast. Digital devices convert selected portions of the analog video signal into digital data, which are compared with data converted previously; if differences exceed preset limits, an alarm is generated.

(2) The signal processor usually provides an adjustable window that can be positioned anywhere on the video image. Available adjustments permit changing horizontal and vertical window size, window position, and window sensitivity. More sophisticated units provide several adjustable windows, which can be indiviually sized and positioned. Multiple windows permit concentrating on several specific areas of an image while ignoring others. For example, in a scene containing six doorways leading into a long hallway, the sensor can be set to monitor only two critical doorways.

4–5. Point Sensors

Point sensors are used to protect specific objects within a facility. These sensors, sometimes referred to as "proximity sensors," detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available, including capacitance sensors, pressure mats, and pressure switches. Other types of sensors can also be used for object protection.

a. Capacitance sensors. These detect an intruder approaching or touching a metal object by sensing a change in capacitance between the object and ground.

(1) A capacitor consists of two metallic plates separated by a dielectric medium. A change in the dielectric medium or electrical charge results in a change in capacitance. In practice, the metal object to be protected forms one plate of the capacitor. The gound plane surrounding the object forms the second plate. The sensor processor measures capacitance between the metal object and the gound plane. An approaching intruder alters the dielectric value, thus changing the capacitance. If the net capacitance change satisfies the alarm criteria, an alarm is generated.

(2) The maximum capacitance that can be monitored by this type of sensor is usually between 10,000 and 50,000 picofarads. The minimum detectable change in capacitance can be as low as 20 picofarads. The signal processor usually has a sensitivity adjustment that can be set so as to detect an approaching intruder several feet away or to require that the intruder touch the object before an alarm is generated.

(3) Because air forms most of the dielectric of the capacitor, changes in relative humidity will affect the sensitivity of the sensor. An increase in humidity causes the conductivity of the air to increase, lowering the capacitance. Conversely, a decrease in humidity reduces the conductivity, resulting in an increase in capacitance. Moving a metal object, such as a file cabinet, closer to or away from the protected object can also affect the sensitivity of a capacitance sensor. Figure 4–8 illustrates a typical application using a capacitance sensor.

b. Pressure mats. Pressure mats generate an alarm when pressure is applied to any part of the mat surface, as when someone steps on the mat. One type of construction uses two layers of copper screening separated by a soft sponge rubber insulation with large holes in it. Another type uses parallel strips of ribbon switches, made from two strips of metal separated by an insulating material and spaced several inches apart. When enough pressure is applied to the mat, either the screening or the metal strips make contact, generating an alarm. Pressure mats can be used to detect an intruder approaching a protected object or can be placed by doors or windows to detect entry. Because pressure mats are easy to bridge, they should be well concealed. One example of concealment is to place them under a carpet.

c. Pressure switches. Mechanically activated contact switches or single ribbon switches can be used as pressure switches. Objects that require protection can be placed on top of the switch. When the object is moved, the switch actuates and generates an alarm. In this usage, the switch must be well concealed. The interface between the switch and the protected object should be so designed that an adversary cannot slide a thin piece of material under the object to override the switch while the object is removed.

4–6. Duress Alarm Devices

These devices, which may be either fixed or portable, are used by operations and security personnel to signal an emergency of a life threatening situation. Activiation of a duress device will generate an alarm at the alarm monitoring station.

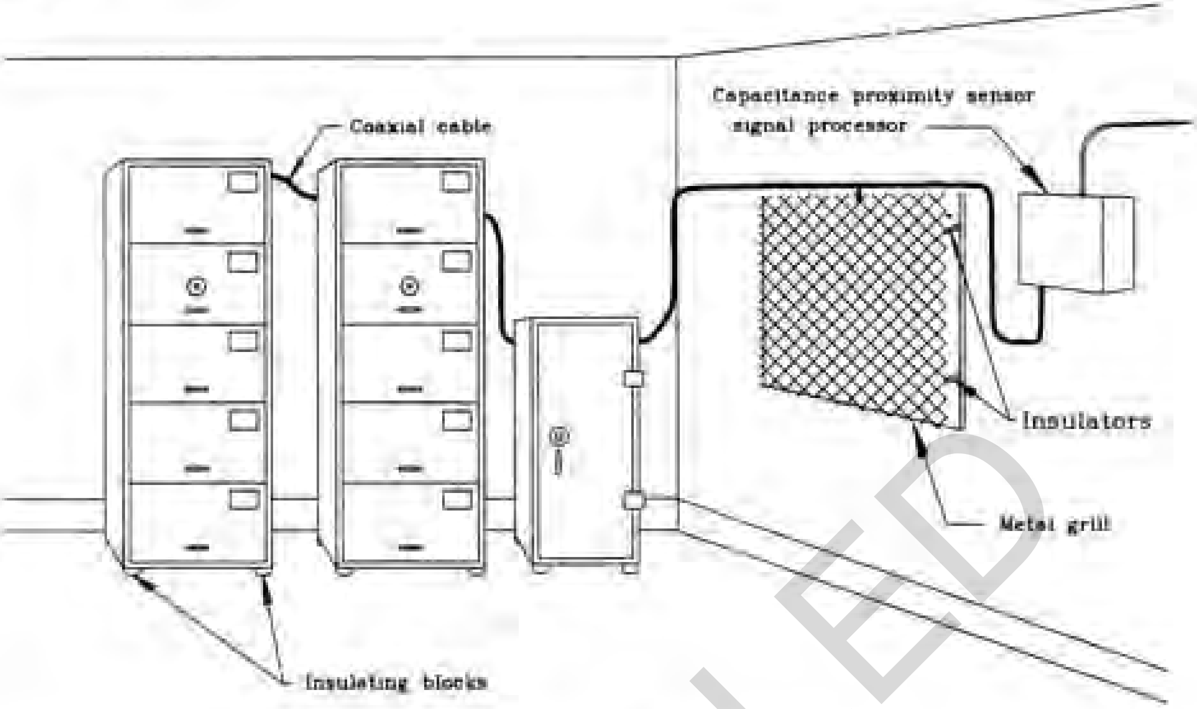


Figure 4-8. Capacitance Proximity Sensor Application.

Because of the nature of the alarm, duress devices should never annunciate at point of threat. Duress devices are customarily manually operated.

a. Fixed. Fixed duress devices are mechanical switches permanently mounted in an inconspicuous location, such as under a counter or desk. They can be simple push-button switches, activated by the touch of a finger or hand, or foot-operated switches attached to the floor.

b. Portable. Portable duress devices are wireless units consisting of a transmitter and receiver. The transmitter is portable and small enough to be conveniently carried by a person. The receiver is mounted in a fixed location within the facility. Either ultrasonic or RF energy can be used as the communication medium. When activated, the transmitter generates an alarm that is detected, if within range, by the receiver. The receiver then activate a relay that is hard-wired to the alarm monitoring system.

Section II. DESIGN GUIDELINES

4-7. Basic Design Criteria

a. Level of security. The type and value of assets within a facility and the anticipated threat determine the level of security required. Refer to TM 5-853-1 for further guidance on determining security level requirements. The security level of each facility can be classified as A, B, C, or D. Appendix B lists security levels recommended for various types of Army facilities; it also includes applicable regulations governing minimum IDS requirements for various types of facilites.

b. Layered protection. An interior IDS can be designed to provide three separate types of detection, consistent with the three general categories of interior sensors: boundary penetration detection, motion detection, and point detection. Refer to TM 5-853-1 and TM 5-853-2 for a detailed discussion of integrating layered detection with barrier systems to provide delay after initial detection. Figure 4-9 is an example of layered IDS detection using only interior sensors. In that figure, structural vibration sensors on walls, glass breakage sensors on the windows, and a balanced magnetic switch on the door provide the first, or penetration, detection layer. (Although not indicated, vibration sensors should also be mounted on the floor and ceiling.) Volumetric sensors mounted on walls provide the second, or motion detection, layer. The innermost layer, that of point detection, is provided by a capacitance sensor monitoring safe and file cabinets. Table 4-2 gives general guidelines for implementing IDS in facilites according to security level.

c. Response and delay time. When dealing with electronic security systems, the response time is defined as the time it takes the security force to arrive at the scene after an initial alarm is

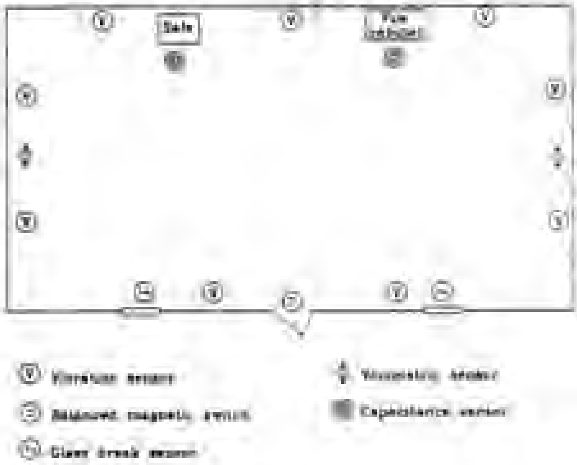


Figure 4–9. Layered IDS Detection.

received at the Security Center. Total delay time is defined as the sum of all the barrier delay times and time required to cross the areas between barriers after an intrusion alarm has been reported, plus the time required to accomplish the mission and leave the protected area.

(1) The basic function of an electronic security system is to notify security personnel that an intruder is attempting to penetrate, or has penetrated, a protected area in sufficient time to allow the response force to intercept and apprehend the intruder. To accomplish this, there must be sufficient physical delay between the point where the intruders are first detected and their objective, to provide delay time equal to or greater than the response time. TM 5–583–1 provides detailed procedures for determining the response time and the required delay time.

(2) When dealing with interior sensors, boundary penetration sensors that detect penetration, such as structual vibration sensors or passive ultrasonic sensors, provide the earliest warning of an attempted penetration. This alarm is usually generated before the barrier is penetrated and therefore provides advance notification to the security force of an attempted penetration, thus allowing the barrier delay time to be counted as part of the total delay time. Door position sensors and glass breakage sensors do not genrate an alarm until after the barrier has been breached, and therefore the delay time provided by the barrier cannot be counted as part of the total delay time.

(3) Volumetric motion sensors do not generate an alarm until the intruder is already inside the area covered by the sensors. Therefore, if these sensors are to be used to provide additional response time, additional barriers must be placed between the volumetric motion sensors and the protected asset.

(4) Point sensors, such as capacitance sensors and pressure mats, provide warning of attempted

Table 4–2. General Guidance for Application of IDS

Detection layer	Security Level Level A	Level B	Level C	Level D
Penetration	BMS on doors and windows 2 layers walls and ceiling (diff tech)	BMS on doors and windows 1 layer walls and ceiling	BMS on doors and windows	BMS on doors and windows
Motion	1 layer (2 if bldg doesn't meet reg req)	1 layer	1 layer (per applicable reg)	
Point	If applicable	If applicable	1 layer on asset to be protected	

penetration only if they detect the intruder before he gains access to the protected asset.

4-8. Layout of Boundary Penetration Sensors

The boundary of an interior area to be protected is usually well-defined by walls, floor, and ceiling. A typical boundary is not homogeneous; it contains a number of doors, windows, and miscellaneous openings, such as vents and utility inlets/outlets. In new construction, careful planning and design coordination can significantly reduce IDS requirements. Usually, several different types of sensors are needed for effective protection of the entire boundary. In all cases, the sensors and associated equipment must be installed inside the boundary.

a. Walls, floor, and ceiling. Structural vibration sensors, passive ultrasonic sensors, and passive audio sensors can detect forcible entry through walls, ceiling, and floor.

(1) Structual vibration sensors should not be used if the walls, floor, and ceiling of the protected area are subject to excessive vibration, such as that caused by large rotating machinery or nearby vehicular traffic. These sensors function quite well on walls constructed of rigid materials, such as reinforced concrete, masonry, solid metal plate, and expanded metal; they should not be used on walls fabricated from plastic or polycarbonate sheets. To perform effectively, the sensors must be firmly attached to the wall's surface. When used to detect penetration of concrete block, cinderblock, or brick structures, it may be necessary to use a steel lattice. The lattice transmits induced vibrations that would otherwise be attenuated in the structure material. The lattice can be made of 1 ½-inch by 3/16-inch galvanized steel, bolted or welded together at overlapping joints. Figure 4-10 shows an example of an installation using a lattice. The number of sensors required is determined by the number of square feet of surface to be protected and the material of which the wall is constructed. The sensors should be positioned near the center of the surface area they protect.

(2) Passive ultrasonic sensors can detect penetration through masonry, concrete, brick, or metal-covered barriers. They are not very effective in detecting penetration through soft materials, such as wood or wall board. These sensors are not attached to the surface of the barrier but are located approximately 20-30 feet away and positioned to face the barrier. The area covered by the sensor is determined by the distance between the sensor and the wall and the adjustment of the sensitivity control. The number of sensors required depends on the size and shape of the structure and the arrangement of furniture and equipment in the area. Because ultrasonic energy is easily

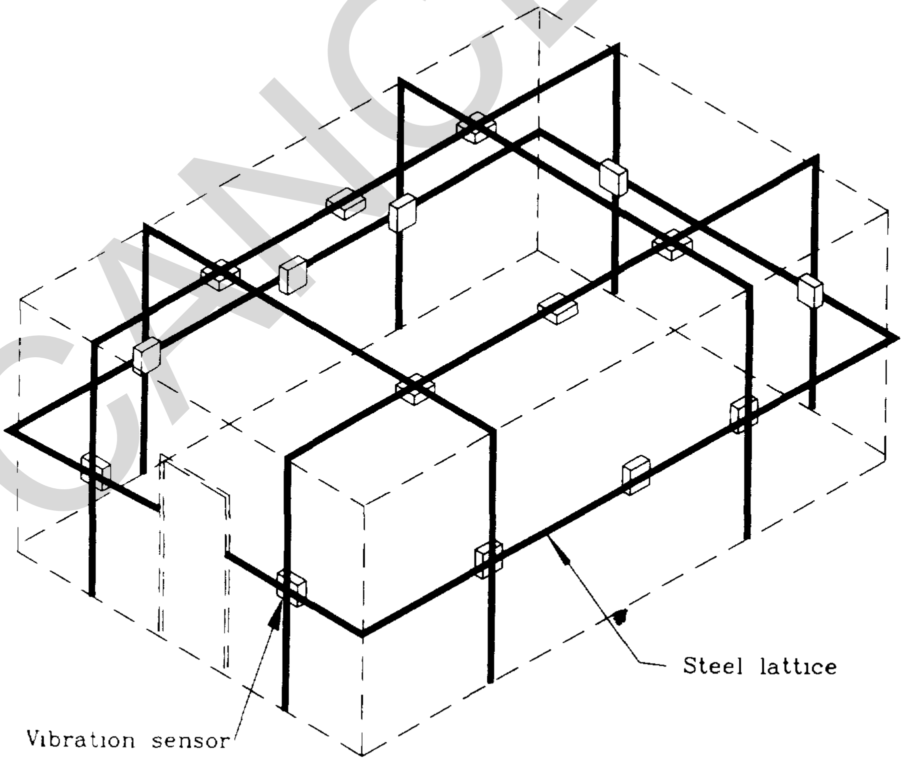


Fıgure 4-10. Installatıon Usıng a Lattıce for Vıbratıon Sensors.

]

blocked by such objects as furniture or cabinets, the sensor must be so located that no objects are between it and the wall. Warning devices (bells and sirens), hissing noises, and squeaky bearings emit ultrasonic energy and may cause nuisance alarms. If possible, these noise sources should be removed or corrected; if not, baffles should be installed around them, to minimize interference with the sensors.

(b) Doors. The door is one of the primary points of attempted penetration into a protected area. Most DOD and Army regulations that include IDS provisions require, as a minimum, that all doors receive IDS protection. This is usually accomplished with balanced magnetic switches. They can be applied to personnel doors, roll up doors, windows, and hatch openings. It should be remembered that these sensors only detect the opening of the door or window; they do not detect an intruder cutting through them. Balanced magnetic switches are available in surface mount and recessed configurations and in many models and style variations. The surface mount configurations are usually used on existing doors and windows. For new construction, the recessed configuration is recommended because it provides inherently more protection against tampering. For doors, the sensor should be mounted at the top and away from the hinges, an arrangement that provides for maximum movement of the magnet when the door is opened. Excessive movement between the switch assembly and the actuating magnet, because of poor fit and misalignment, can result in nuisance alarms. Any misaligned doors and windows should be adjusted and tightened before installation of this type of sensor. Figure 4–11 shows a typical balanced magnetic switch installation.

c. Windows. The breakage of glass by an intruder attempting to enter a protected area can be detected using glass breakage sensors. A variety of glass breakage sensors is available. Some require external dc power; others have built-in batteries. Some feature a built-in alarm relay; others provide an analog output signal monitored by a separate control unit containing the alarm circuitry. The number of sensors required depends on the size and number of windows to be protected. A single sensor can typically protect about 100 square feet of glass. However, the detection range is considerably reduced for multiple panes of glass because high frequencies are attenuated by the window frames. The sensors are usually mounted in the corner of the window, approximately 2 inches from the edge of the frame, and are bonded to the glass with an adhesive. The adhesive must withstand long exposures to sunlight, heat, cold, and moisture condensation.

d. Miscellaneous openings. Openings in the wall or ceiling are often overlooked. All openings where the shortest dimension is more than six inches and that are greater than 96 square inches in area should be provided with IDS protection. If the openings are equipped with removable access covers, balanced magnetic switches can be used. Metal grills or security screens containing a grid wire sensor can be used to cover an opening. Openings that are seldom used can be covered with a metal plate equipped with a vibration sensor.

4–9. Layout of Volumetric Motion Sensors

Volumetric sensors detect intruder motion within a confined space. They are usually positioned so that their detection patterns completely cover the

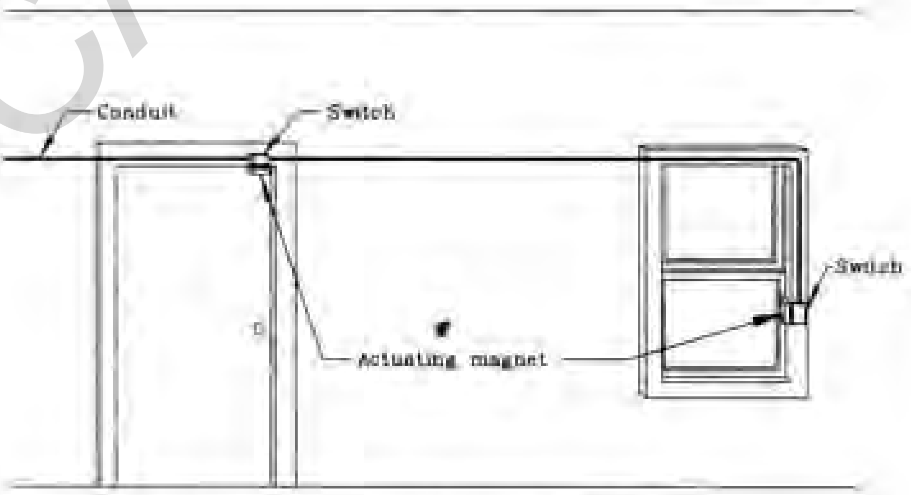


Figure 4–11. Typical Balanced Magnetic Switch Installation.

enclosed area. However, they can also be used as boundary penetration sensors or point sensors if positioned so that their detection patterns encompass the walls, floor, ceiling, or object to be protected. The size and configuration of the area to be protected, arrangement of equipment and furniture within the area, detection pattern limitations influence the number and locations of sensors required. Factors the designer must consider in selecting an appropriate motion sensor, determining the number required, and their effective placement are discussed in the following paragraphs.

a. General considerations. In selecting a volumetric motion sensor, the following characteristics should be considered.

(1) *Detection pattern.* The detection pattern of a motion sensor is determined by its field of view and its range of detection.

(*a*) The field of view is the horizontal and vertical angular coverage the sensor provides. For active sensors, configuration of the transmitting element or antenna determines the vertical and horizontal coverage. For passive sensors, this is determined by the number and shape of lenses or reflectors. A wide variety of fields of view is available for each of the different types of motion sensors. A designer must decide whether to select one sensor with a large field of view or mulitple sensors with smaller fields of view. A single sensor is less costly; however, mulitple sensors can be used to create a patterned zone of detection.

(*b*) *Range of detection.* How far a motion sensor can "see" is known as its range of detection, or operating distance. It can depend on the sensor's height, the size of the target, and the speed, or velocity, of the target. For active sensors, the sensitivity, or range adjustment, also determines the effective range.

(2) Direction of movement. A motion sensor's probability of detection is dependent on the direction of the intruder's movement. For active sensors, motion directly toward or away from a sensor produces a larger Doppler shift than motion at right angles to the field of view. On the other hand, passive infrared sensors are more sensitive to motion at right angles to the sensor's field of view than to motion directly toward or away from the sensor. The anticipated direction of an intruder's movement should always be considered when selecting or positioning motion sensors for a specific area.

(3) *Velocity.* A sensor's probability of detection is also dependent on the velocity at which the intruder moves within or through a detection zone. For active sensors, the velocity of a moving object influences the magnitude of the Doppler shift. The higher the velocity, the greater the shift. If an object's velocity is too low, the Doppler shift may not be large enough to satisfy the sensor's alarm criteria. On the other hand, if the velocity is too high, the resultant frequency shift may be outside the limits of the sensor's input filter and, therefore, not detectable. Although passive sensors detect changes in thermal radiation, their alarm criteria also include the rate of change of the thermal radiation. The circuitry includes upper and lower limits that define a velocity range within which an intuder can be detected. Volumetric motion sensors should be able to detect a standard intruder moving within the sensor's detection pattern at velocities of between 0.3 and 7.5 feet per second.

(4) *Resolution.* The smallest detectable displacement of an object that can be recognized by a sensor is known as its resolution. It is usually measured in angular degrees. However, this parameter is seldom specified in the manufacturer's data sheets. From a more practical viewpoint, the sensor should be able to detect a standard intuder moving within a specifed velocity range before the intruder reaches his goal.

(5) *Nuisance alarms.* Of the three categories of interior sensors, volumetric motion sensors are the most prone to nuisance alarms. Sources that have been identified as common causes of nuisance alarms for ultrasonic, microwave, and passive infrared motion sensors are listed in table 4-3.

b. Layout of ultrasonic motion sensors. The following factors should be considered in determining the number and placement of ultrasonic motion sensors needed to provide adequate protection of an area.

(1) Extraneous ultrasonic energy sources, both within and outside the area to be protected, should be identified. If possible, outside sources should be removed or the area to be protected should be sealed or isolated so as to minimize outside interference. Internal sources, such as hissing steam pipes, ringing bells, and squeaky machine bearings, should be eliminated or baffled to minimize nuisance alarms.

(2) Ultrasonic sensors should not be used in areas with high volumes of moving air. Air turbulence can distort the energy pattern, causing numerous nuisance alarms. In areas with normal air turbulence, caused by heating, ventilating, and air conditioning systems, the sensors should be located away from the vents. If it is necessary to locate a sensor close to a vent, baffles should be installed to deflect the air away from the sensor's field of view. However, care should be exercised so as not to interfere with air flow to the point that it causes discomfort for the occupants. In areas

Table 4-3. Common Causes of Nuisance Alarms in Volumetric Sensors

Cause	*Ultrasonic*	*Microwave*	*Infrared*
1. Air turbulence			
a Fluttering venetian blinds	yes	yes	no
b Fluttering curtains and drapes	yes	no	no
c Fluttering metallic decorations	yes	yes	no
d. Escaping air or stream	yes	no	no
2. Noise			
a. Warning devices (sirens, bells)	yes	no	no
b. Clocks and chimes	yes	no	no
3. Electrical			
a. Transformers	no	yes	yes
b. Arcing	no	yes	yes
c. Fluorescent lights	no	yes	no
d. Lightning	yes	yes	yes
4. Vibration			
a. Heavy machinery	yes	yes	no
b. Heavy thunder	yes	yes	no
c Seismic phenomena	yes	yes	no
5. Miscellaneous			
a. Humidity	yes	no	yes
b. Rodents or other animals	yes	yes	yes
c. Heat sources	no	no	yes

where moderate air turbulence cannot be eliminated, adequate coverage can be provided by increasing the number of sensors and reducing their sensitivity.

(3) Room acoustics are important in determining the number of sensors required for adequate coverage. Hard surfaces, such as masonry, metal, and glass, in the sensor's field of view tend to increase a sensor's sensitivity and, consequently, its range of detection. Soft, nonreflecting surfaces, such as carpets or drapes, absorb ultrasonic energy, thus reducing sensitivity and decreasing the effective detection range.

(4) To maximize the Doppler-shifted signal and enhance detection capability, sensors should be positioned so that the transmitted energy is directed toward the most probable intruder entry point or route through the protected area.

(5) As previously noted, ultrasonic motion sensors are available in two basic packaging configurations: transceivers or separate transmitter and receiver units. The selection or one of the other depends on the size and shape of the area to be protected, the arrangement of equipment within the area, and designer or user preference.

(*a*) Transceivers are typically mounted on walls, although they can be mounted on ceilings if required. When multiple transceivers are used, the detection patterns should be overlapped to avoid dead spots, that is, unprotected areas. However, transceivers should never be pointed towards each other. Interference of the energy patterns of individual transceivers can reduce the effective range of each transceiver as well as create nuisance alarms. Examples of how ultrasonic transceivers can be positioned to provide coverage are shown in figure 4-12.

(*b*) Ultrasonic sensors consisting of separate transmitters and receivers are typically mounted on ceilings. As with transceivers, the individual transmitters and receivers should be positioned to preclude dead spots and to cover those areas where an intruder is most likely to enter or move. Examples of positioning ceiling-mounted ultrasonic transmitters and receivers are shown in figure 4-13.

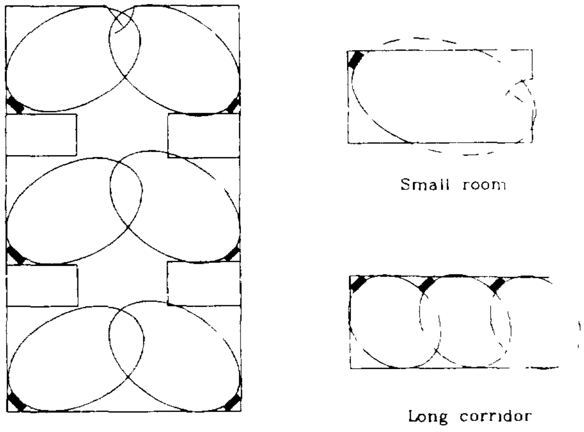


Figure 4-12. Placement of Ultrasonic Transceivers.

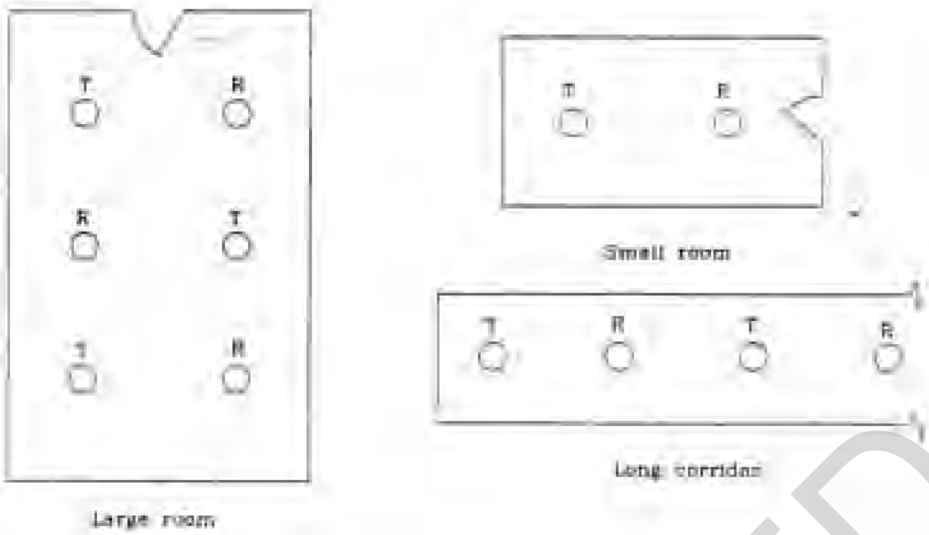


Figure 4–13. Placement of Ultrasonic Transmitters and Receivers.

c. Layout of microwave motion sensors. Factors to be considered in determining placement of microwave motion sensors include the following:

(1) The shape of the detection pattern of a microwave sensor is determined by antenna configuration. Antennas are available that generate omnidirectional and directional energy patterns. Omnidirectional antennas generate circular or hemispheric energy patterns, whereas directional antennas generate broad or narrow teardrop-shaped patterns. Omnidirectional sensors are usually mounted on the ceiling and directional sensors on the wall. The effective detection range of a sensor can be controlled with the sensitivity adjustment. Hence, the number of sensors required and their placement are determined to a large extent by the antenna configuration selected by the designer.

(2) Radiated energy from microwave sensors can, to some degree, penetrate walls, windows, and doors of nonmetallic structures. The degree of penetraion is dependent on the frequency of transmitted energy and type of material it must penetrate. Generally, the lower frequency results in greater penetrating ability. Dense materials, such as concrete and brick, provide greater penetration resistance than glass or wood. It is good practice not to point directional sensors toward an exterior wall, especially if there are large, moving metal objects outside the wall that can reflect enough energy back through the wall to cause an alarm.

(3) Arrangement of furniture and equipment within the area must also be considered. Microwave energy can penetrate wooden furniture and wooden or glass partitions. However, it does not penetrate metal furniture, file cabinets, and metal partitions. In fact, metal surfaces reflect microwave energy in much the same way that mirrors reflect light. Accordingly, the designer must be careful in positioning microwave sensors; their energy should not be directed toward a wall or object so that reflected energy causes detection of movement outside the protected area.

(4) Because air is not used as the medium for transmitting microwave energy, microwave sensors are not affected by air turbulence as are ultrasonic sensors. However, large metal surfaces, such as thin metal warehouse walls or an overhead door, moving in wind or air turbulence, can cause false alarms. Also, rotating machinery, rotating fan blades, and movement of metal holiday ornaments are potential sources of false alarm. Fluorescent lights can be particularly troublesome because the on/off ionization cycle of the lamps is within the frequency range of the Doppler shift cause by motion of a human intruder.

(5) As with ultrasonic sensors, microwave sensors rely on the Doppler effect to detect intruder motion. Hence, they should be so positioned that the transmitted energy is directed toward the most probable intruder entry point or route through the protected area.

d. Layout of passive infrared motion sensors- . The following factors should be considered in determining how many of these sensors are needed and how they should be placed to provide adequate coverage of an area.

(1) The detection pattern of infrared sensors is determined by the lens or mirror assembly used to monitor thermal radiation. Infrared sensors provide the greatest flexibility of the three common types of volumetric motion sensors in the choice of a detection pattern most suitable to a specific application. Sensors are available with very nar-

row or wide angular fields of view and short or long detection distances. Sensors that monitor a hallway and up or down a stairwell are available, as well as sensors that can provide a long narrow vertical column of protection. A careful evaluation of available detection patterns can minimize the number of sensors required and provide more optimum coverage of the area.

(2) Unlike ultrasonic or microwave sensors, infrared sensors are more sensitive when positioned so the expected intruder path is at right angles to the sensor's field of view. Also, unlike ultrasonic or microwave sensors, infrared sensors can be mounted facing each other. Not only does this allow more effective overlap of detection patterns, it also provides additional protection against tampering with sensors. Examples of correct placement of passive infrared sensors are depicted in figure 4–14.

(3) Passive infrared sensors are not affected by environmental conditions, such as humidity, air currents, and acoustic disturbances. Because these sensors do not transmit energy, they are not sensitive to building vibrations. However, care is still necessary in positioning the sensors. Rapid changes in temperature of stationary objects in the area can sometimes cause alarms. For example, failure of a light bulb or on and off cycling of a space heater may generate an alarm. Sensors should be positioned so that such devices are not within their field of view. They should not be located near heat sources, such as radiators, heaters, and hot pipes, that could produce thermal gradients in front of the sensor lens. These sensors suffer reductions in range and sensitivity when ambient termperatures are 95 degrees Fahrenheit or higher.

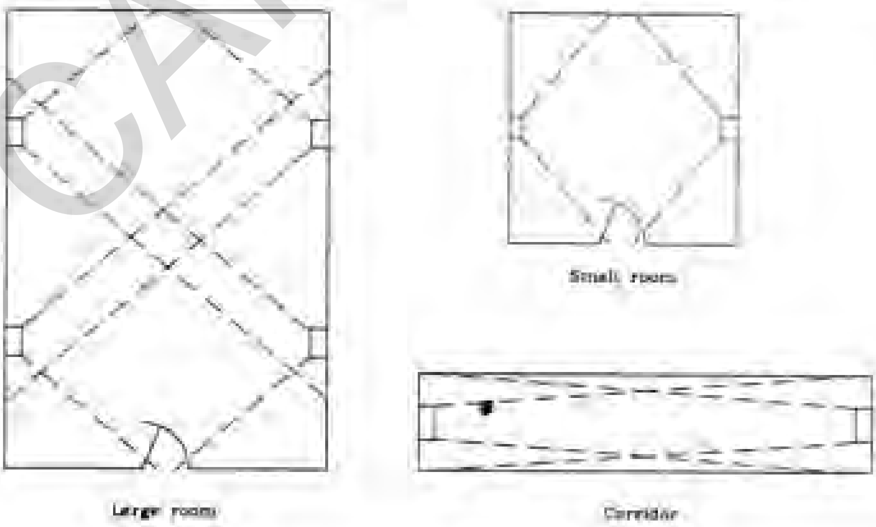
e. Layout of video motion sensors. The following factors should be considered in determining the number and placement of video motions sensors needed to provide adequate coverage of a protected area.

(1) A sufficient number of cameras should be provided to ensure that the entire protected area is covered by the combined fields of view. Complete coverage permits adequate visual assessment in response to alarms generated by video motion sensors.

(2) Sensor detection windows should be adjusted to avoid areas of motion that might trigger nuisance alarms. The windows should cover assets to be protected and possible entryways that can be used by an intruder. Because these sensors are sensitive to changes in contrast or brightness, detection windows should be positioned to avoid changes in illumination levels, such as the shining of moving vehicle headlights through a window.

(3) Care must be used in setting the manual sensitivity adjustment. It must be adjusted to be sensitive enough to detect standard intruder motion but not so sensitive that small contrast or lighting changes or movement of small animals will cause nuisance alarms.

(4) Because video motion sensors process and compare successive camera images, cameras must be mounted on vibration-free surfaces so that image differences caused by camera movement do not occur. Such movement can result in the generation of nuisance alarms.



Large room

Small room

Corridor

Figure 4–14. Placement of Passive Infrared Sensors.

4-10. Layout of Point Sensors

Point sensors can detect touching or lifting an object within a protected area. Capacitance sensors usually provide more effective protection of metal objects, such as safes or file cabinets, than pressure mats or switches. They can also detect penetration attempts through metal grids placed over the inside of windows, vents, and other openings. All objects to be thus protected must be isolated from ground. Metal safes and filing cabinets can be isolated by placing them on insulated mounts; metal grids can be attached to window frames with insulated stand-offs. Insulators made of nonconductive plastic or nonhydroscopic material should be used. Wood should not be used because it may absorb enough moisture over a period of time to change the dielectric value. A single capacitance sensor can be used to protect a series of objects, so long as the combined capacity does not exceed the maximum capacity of the sensor. Typical safes and filing cabinets have a capacitance of approximately 500 picofarads. Because the sensor monitors the capacitance between the protected objects and ground, an adequate ground plane is essential. If an adequate ground plane does not exist, a reference ground plane can be established by placing an electrically grounded metal sheet or foil on the floor under the object. In applications where the object itself must be grounded, an insulated blanket with an embedded conductive layer can be draped over the object. Movement of the blanket should generate an alarm.

4-11. Additional Sensor Considerations

Additional factors to be considered when planning and laying-out an interior IDS include tamper protection, access/secure mode capability, remote-test capability, local alarm indicator lights, signal wiring, and economics.

a. Tamper protection. To minimize the possibility of someone tampering with circuitry and associated wiring, all sensor-related enclosures must be equipped with tamper switches. These switches must be positioned so that an alarm is generated before the cover has been moved enough to permit access to the circuitry of adjustment controls. In addition, several types of sensors should be equipped with tamper switches to protect against being repositioned or removed. Security screens containing grid wire sensors and vibration sensors that can be easily removed from a wall are examples of sensors that require tamper switches.

b. Access/secure mode. During regular working hours, many of the interior sensors must be deactivated by placing the area(s) in the access mode. For example, door position sensors and volumetric sensors in areas that are occupied must be deactivated to prevent generation of multiple nuisance alarms caused by the normal movement of people. This can be done locally or remotely. With local control, a switch is used to bypass or shunt alarm contacts when the sensor is placed in the access mode. When done remotely, the Security Center operator usually enters a command that causes the processor software to ignore incoming alarms from those sensors placed in access. However, when a sensor is placed in the access mode, the sensor's tamper protection circuitry must remain in the activated, or secure, mode. After working hours, when the facility is unoccupied, all sensors must be again placed in the secure mode. Certain devices, such as duress alarm switches, tamper switches, grid-wire sensors covering vent openings, and glass breakage sensors, should never by placed in the access mode. The designer must ensure that selected sensors can be placed in an access mode, if required, and that certain types of sensors, such as duress and tamper switches, are configured so that they cannot be put in access under any condition.

c. Remote-test capability Many sensors can be provided with a remote-test capability to verify operation of the sensor circuitry. Some, but not all, sensors that incorporate a remote-test feature use devices that actuate (or upset) the same sensor phenomenology as would an actual intruder. For example, balanced magnetic switches can be provided with an internal coil that, when activated, can disrupt the normally balanced magnetic fields sufficiently to generate an alarm. Volumetric motion sensors can be tested with external stimuli that generate a signal representative of a human intruder. These test units are normally mounted on a wall opposite the sensor. Other sensors have limited remote-test capabilities; that is, only a portion of the sensor, such as the signal processor, is tested. Army regulations require that sensors in certain applications must be tested at least monthly by opening the door or causing actual alarms. Sensors using remote test features that actuate the sensing phenomenology will meet these requirements. When remote test capabilites are used, a more frequent test schedule can be implemented, usually once or more per day. This higher test rate provides a higher level of confidence of system integrity than testing manually on a once per month basis. Sensors with limited remote-test capabilities can be used if they are supplemented with test procedures that include manual testing of sensor phenomenology.

d. Alarm indicator light. Many interior sensors have an alarm indicator light, activated when the sensor initiates an alarm. This feature is quite useful during installation and maintenance operations. The sensitivity can be adjusted, and the sensor can be tested without monitoring the control unit's output. However, the light may also warn intruders that they have been detected. Insiders may also be able to study the detection pattern to identify dead zones in which one may escape detection. To correct these problems, a switch must be provided that can be used to deactivate the light during normal operation.

e. Signal wiring. The designer must consider two types of signal circuit paths when implementing an interior IDS: the path between a detector and its signal processor and the path between the signal processor alarm output circuitry and the local processor. In some cases, the signal processor and detector are in the same enclosure. Some sensors, such as door position switches and manual duress switches, do not have a signal processor; they are wired directly to the local processor.

(1) *Detector to signal processor.* Shielded twisted pairs, coaxial cable, or both are typically used to connect a detector to its signal processor. Usually, low-level analog signals and dc power are transmitted over the link. Because the detector and the signal processor are both normally mounted within the protected area, line supervision is usually not required. All cabling must be routed in rigid galvanized steel conduit.

(2) *Signal processor to local processor.* The alarm signal from a signal processor is usually in the form of a relay contact closure. Under usual conditions, the contact is normally closed; however, when an alarm is generated, the contact opens. With this arrangement, an alarm is generated if someone cuts the wires or the wires are accidentally disconnecetd. Twisted pairs (wire lines) are normally used to connect the sensor's relay output to the alarm-monitoring equipment, such as a local processor. Because it is relatively easy to electrically short a twisted pair, simulating a no-alarm condition, and because the sensor may be located some distance from the alarm monitoring equipment, it is essential that some form of data link security be provided. Chapter 9 describes various line supervision techniques. All wiring must be routed through conduit. If wiring leaves the protected area, rigid galvanized steel conduit must be used.

f. Economic considerations. The cost of an interior IDS depends on the size of the area to be protected, the number of layers of IDS protection required, and types of sensors to be used. Costs for installing the sensors, including labor and material (conduit and wiring), typically exceed the sensor's cost. Detailed cost estimating data can be found in other agency documentation.

CHAPTER 5

EXTERIOR INTRUSION DETECTION SENSORS

Section I. TYPES OF SENSORS

5-1. General

Exterior intrusion detection sensors are customarily used to detect an intruder crossing the boundary of an area being protected. They can also be deployed in clear zones between fences or around buildings. They can also be applied to protection of materials and equipment stored outdoors within a protected boundary or to perimeter detection for buildings and other facilities.

a. Exterior sensors are designed to operate in an outdoor environment; they must perform reliably while exposed to environmental conditions. The detection function must be performed with a minimum of unwanted alarms, such as those caused by wind, rain, ice, standing water, blowing debris, animals, and other sources. See chapter 4 for definition of alarm types.

b. Important criteria to be considered in selection of exterior sensors are probability of detection, susceptibility of the sensor to unwanted alarms, and vulnerability of the sensors to defeat.

(1) The PD of an exterior sensor is much more vulnerable to the physical and environmental conditions of a site than is an interior sensor. Many uncontrollable forces, such as wind, rain, fog, ice, frozen soil, standing or running water, falling and accumulated snow, and blowing dust and debris, may affect an exterior sensor's performance and cause a dramatic drop in the PD.

(2) In general, because of the nature of the outdoor environment, exterior sensors are also more susceptible to nuisance and environmental alarms then interior sensors. Inclement weather conditions (heavy rain, hail, and high wind), vegetation, blowing debris, and animals are major sources of unwanted alarms.

(3) As with interior sensors, tamper protection, signal line supervision, self-test capability, and proper installation make exterior sensors less vulnerable to defeat. Because signal processing circuitry for exterior sensors is generally more vulnerable to tampering and defeat than signal processing circuitry for interior sensors, it is extremely important that enclosures are located and installed properly and that adequate physical protection is provided.

c. Several different types of exterior intrusion detection sensors are available. They can be categorized as—.

(1) Fence sensors.

(2) Buried line sensors.

(3) Line-of-sight sensors.

(4) Video motion sensors.

5-2. Fence Sensors

Fence sensors detect attempts to penetrate a fence around a protected area. Penetration attempts, such as climbing, cutting, or lifting, generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain. Five basic types of sensors are used to detect these vibrations and stresses: mechanical, electromechanical, strain-sensitive cable, taut wire, and fiber optic. Other types of fence sensors detect penetration attempts by sensing changes in an electric field or in capacitance.

a. Mechanical fence sensors. All sensors of this type depend on movement of the fence to cause a switch mechanism to open or close a set of contacts. Two basic approaches are generally taken: one uses a mechanical inertia switch, the other a mercury switch.

(1) In the inertia switch, a metallic mass rests on a set of electrical contacts. Movement of the switch causes the mass to bounce, momentarily opening and closing the contacts. Movement of the mass may be unrestricted or restricted by a spring or magnet. An unrestricted mass is more sensitive to fence movement; however, it is also more prone to generate unwanted alarms.

(2) The mercury switch consists of a glass vial containing a small amount of mercury with a set of normally open electrical contacts located close to, but not immersed in, the mercury. Movement of the switch displaces the mercury, momentarily shorting the contacts.

(3) A pulse counting circuit in the signal processor for these switches recognizes a momentary contact opening or closing as a single pulse. The number of pulses generated by the switch and the pulse rate depend on the method of attack and time required for the intruder to penetrate the fence. When the number of pulses satisfies the count and time criteria, an alarm is generated.

(4) The switches may be mounted on fence posts or attached directly to the fabric. Typically, they are spaced anywhere from 10 to 30 feet apart.

As many as 50 switches can be wired to one signal processor. Figure 5-1 shows an example of a mechanical fence sensor installation.

b. Electromechanical fence sensors. These sensors use transducers that generate an analog electrical signal in response to mechanical vibrations caused by an attempted penetration of the fence. Two types of transducers are in common use: piezoelectric and geophone.

(1) Piezoelectric transducers contain a piezoelectric crystal shaped to respond to vibrational frequencies generated in a fence during an intrusion. The crystal produces an analog signal that varies in amplitude and frequency with the amplitude and frequency of the mechanically induced vibrations.

(2) Geophone transducers operate on the principle of a conducting loop moving in a fixed magnetic field. Disturbing the fence causes movement of the loop, generating an analog signal proportional in amplitude and frequency to the mechanically induced vibration.

(3) For both types of transducers, the signal processor usually contains a bandpass filter that passes only those frequencies characteristic of the vibrations generated during an attempted penetration of a fence. Filtering reduces susceptibility to false alarms that could result from low-frequency vibrations induced by low-velocity winds. When characteristics of the signal, such as amplitude, frequency, and duration, satisfy the processor's criteria, the sensor initiates an alarm.

(4) Depending on the manufacturer's model, these transducers can be mounted on fence fabric or posts and can be spaced 10 to 30 feet apart. As many as 50 or more transducers can be electrically wired in parallel to one signal processor.

c. Strain-sensitive cable. These cables are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subjected to mechanical distortions or stresses resulting from fence motion. Three types of strain sensitive cable are available.

(1) The electret type is a coaxial cable in which dielectric material between the center and outer conductors has been processed (by applying a high polarizing voltage to the dielectric when it is heated to near the melting point) to retain a permanent electrostatic charge. Minute movement of the cable generates an analog signal.

(2) Another type of cable uses the triboelectric effect to produce an analog voltage in response to movement of the cable.

(3) The third type consists of two continuous semicircular permanent magnets extruded from a flexible magnetic polymer. Two insulated conductors maintain an air gap between the magnets. Movement of the cable at any point along its length causes the conductors to move in the air gap in relation to the magnetic field, resulting in generation of an analog voltage.

(4) Strain sensitive cables are sensitive to both low and high frequencies. The signal processor usually has a bandpass filter that passes only those signals characteristic of fence penetration actions. When frequency, amplitude, and duration characteristics of the signal satisfy the processor's criteria, an alarm is initiated.

(5) Because each type of cable acts like a microphone, some manufacturers offer an option that allows the operator to listen to fence noises causing the alarm, to determine whether they are naturally occurring sounds from wind or rain or are from an actual intrusion attempt. This feature is relatively costly to implement because it requires additional cable from each signal processor to the Security Center, and if CCTV is being used, it may be of limited benefit.

(6) Strain-sensitive cable is attached to chain-link fence about halfway between the bottom and

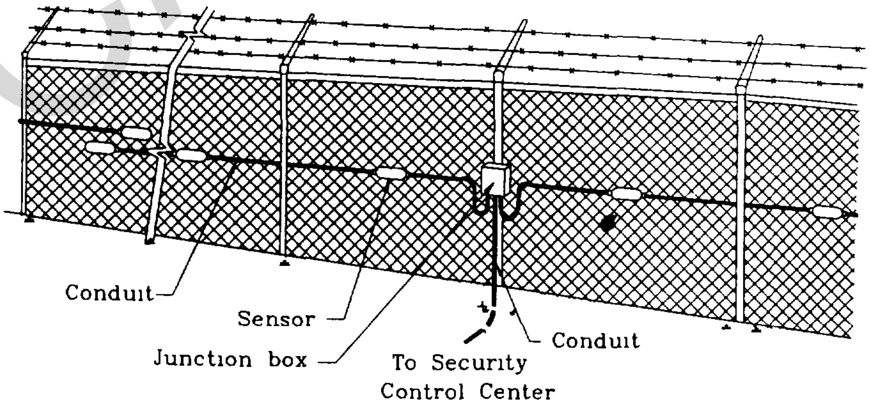


Figure 5-1. Example of Mechanical Fence Sensor Installation

top of the fence fabric with plastic ties. One end of the cable is terminated at the signal processor and the other end with a resistive load. Direct current through the cable provides line supervision against cutting or electrically shorting the cable or disconnecting it from the processor. A typical installation is shown in figure 5-2.

d. Taut wire sensor. This device combines a physically taut wire barrier with an intrusion detection sensor network. The taut wire sensor consists of a column of uniformly spaced horizontal wires, up to several hundred feet in length, securely anchored at each end. Typically, the wires are spaced 4 inches to 8 inches apart. Each is individually tensioned and attached to a detector located in a sensor post.

(1) Two types of detectors are in common use: mechanical switches and strain gauges.

(*a*) The mechanical switch consists of a specially designed switch mechanism that is normally open. The tensioned wires are mechanically attached to the switch, and movement of the wire beyond a preset limit causes the switch to close. To counteract small gradual movements of a wire, such as may be caused by settling of the fence or by freezing or thawing of soil, switches are usually supported in their housing by a soft plastic material. This material allows the switch to self-adjust when acted upon by gradual external forces.

(*b*) Strain gauge detectors are attached to the taut wire by means of a nut on a threaded stud. Whenever a force is applied to the taut wire, the resulting deflection is converted by the strain gauge into a change in electrical output that is monitored by a signal processor.

(2) With sensors that use mechanical switches as detectors, the switches in a single sensor post assembly are wired in parallel and connected directly to the alarm annunciation system. Pulse count circuitry is not used because a single switch closure, such as caused by an intruder moving or cutting one wire, is indicative of an intrusion attempt. Strain gauge detectors in a sensor post are monitored by a signal processor. When the signal from one or more strain gauges satisfies the processor's criteria, an alarm is initiated.

(3) The taut wire sensor can be installed as a free-standing fence or can be mounted on an existing fence or wall. Figure 5-3 depicts a free-standing configuration.

e. Fiber optic cable sensors. This sensor consists of a column of steel tapes strung horizontally across fence posts or outriggers. Optical fibers through which light passes are embedded in each tape. Any break in the fiber optic strand caused by climbing or cutting interrupts the light, resulting in an alarm. Like taut wire, the tapes can be mounted to posts to serve as a stand-alone fence or be attached to an existing fence or wall.

f. Electric field sensors. This type of sensor consists of an alternating current field generator, one or more field wires, one or more sense wires, and a signal processor. The generator excites the field wires, around which an electrostatic field pattern is created. The electrostatic field induces electrical signals in the sense wires, which are monitored by the signal processor. Under normal operating conditions, the induced signals are constant. When an intruder approaches the sensor, however, the induced electrical signals are altered, causing the signal processor to generate an alarm.

(1) Several different field- and sense-wire configurations are available. They range from one field wire and one sense wire to as many as four field wires and four sense wires. Figure 5-4 shows the detection pattern produced by vertical three-wire (one field and two sense wires) and four-wire (two field and two sense wires) configurations. The three-wire system has a wider detection envelope and is less costly (one less field wire and associ-

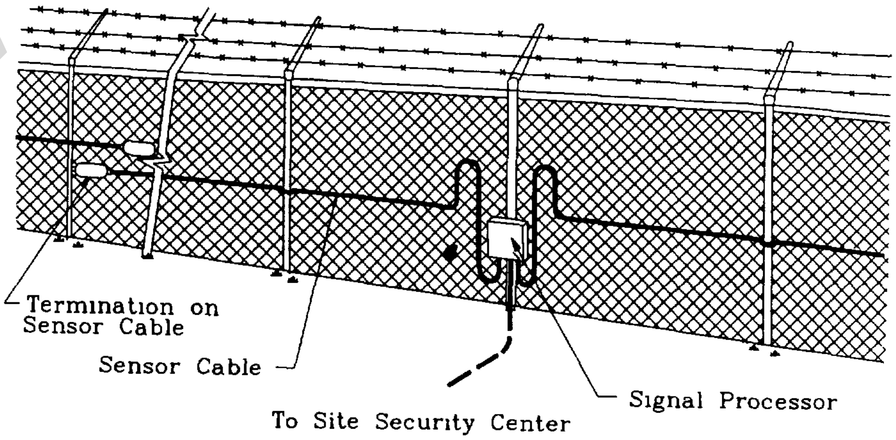


Figure 5-2. Typical Strain Sensor Cable Installation.

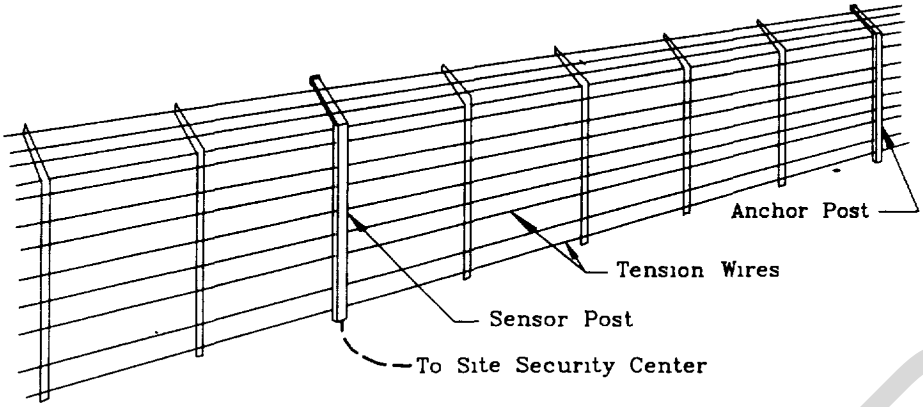


Figure 5–3. Typical Taut Wire Installation.

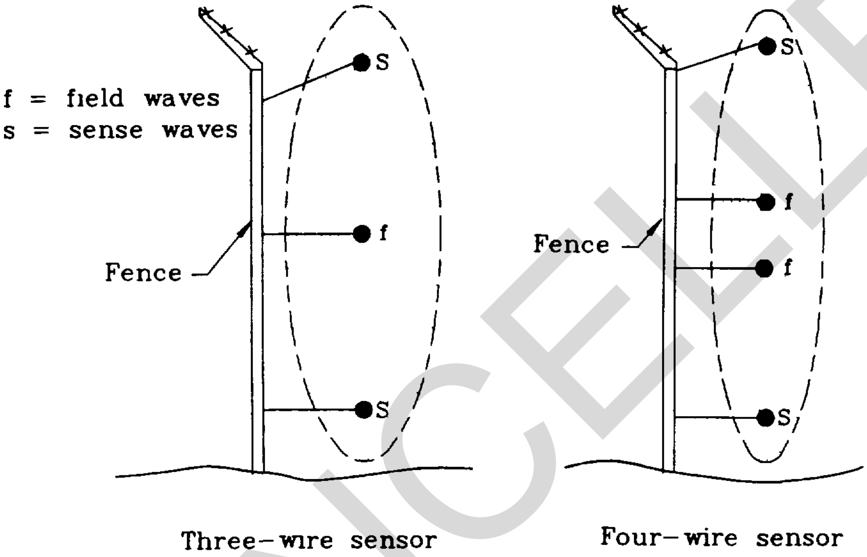


Figure 5–4. Typical Electric Field Sensor Detection Patterns.

ated hardware). However, because of the tighter coupling between wires, the four-wire system is less susceptible to nuisance alarms caused by extraneous noise along the length of the zone.

(2) A signal processor monitors signals produced by the sense wires. The processor usually contains a bandpass filter that rejects high frequency signals, such as those caused by wind vibrating the field and sense wires, and low frequency signals, such as those caused by objects striking the wires. Additional criteria that must be satisfied before the processor initiates an alarm include signal amplitude and signal duration. By requiring the signal to be present for a preset period of time, false alarms, such as those caused by birds flying through the detection pattern, can be minimized.

(3) As with taut wire sensors, electric field sensors can be free standing (mounted on their own posts) or attached by standoffs to an existing fence. They can be configured to follow contours of the ground. The area under the sensor must be clear of vegetation, since vegetation near or touching sense wires can cause false alarms. These sensors can also be installed on the walls and roof of a building.

g. Capacitance proximity sensors. These sensors measure the electrical capacitance between earth ground and an array of sense wires. Any variation in capacitance, such as that caused by an intruder approaching or touching one of the sense wires, initiates an alarm.

(1) These sensors usually consist of two or three wires attached to outriggers along the top of an existing fence, wall, or roof edge. Multiwire versions of up to 11 wires are also available and are either attached to existing fence posts or configured as a stand-alone system. Figure 5–5

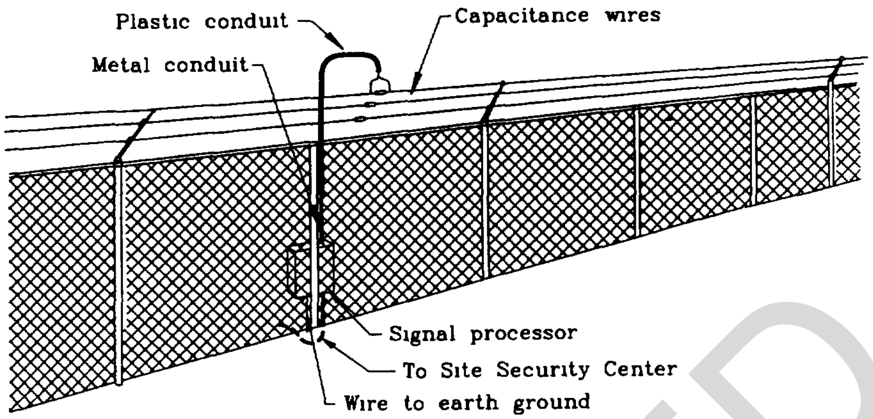


Figure 5–5. Typical Capacitance Sensor Configuration

shows a typical capacitance sensor consisting of three sensor wires attached to the outrigger of a fence.

(2) To minimize environmental alarms, the capacitance sensor is divided into two arrays of equal length. The signal processor monitors the capacitance of each array. Changes in capacitance common to both arrays, such as produced by wind, rain, ice, fog, and lightning, are canceled within the processor. However, when changes occur in one array and not the other, because of an intruder, the processor initiates an alarm.

(3) The multiwire, or full fence, version of the sensor is susceptible to nuisance alarms caused by movement of nearby vegetation. To minimize these alarms, it is necessary to remove or control the growth of vegetation for several feet on each side of the sensor.

5–3. Buried Line Sensors

A buried line sensor system consists of detection probes or cable buried in the ground, typically between two fences that form an isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm if an intruder passes through the detection field. Buried line sensors have several significant features: (1) they are hidden, making them difficult to detect and circumvent; (2) they follow the natural contour of the terrain; and (3) they do not physically interfere with human activity, such as grass mowing or snow removal. However, buried line sensors are affected by certain environmental conditions, such as running water and ground freeze-/thaw cycles. Of the different types of buried line sensors, such as ported coax cable, seismic, seismic/magnetic, magnetic, and balanced pressure, only the ported coax cable is currently used for perimeter protection at Army facilities.

a. The ported coax cable sensor consists of two coaxial cables buried in the ground parallel to each other. An RF transmitter is connected to one cable and a receiver to the other. The outer conductor of each cable is ported (fabricated with small holes or gaps in the shield). The transmitter cable radiates RF energy into the medium surrounding the cables. A portion of this energy is coupled into the receiver cable through its ported shield. (Because of the ported shields, these cables are frequently referred to as "leaky" cables.) When an intruder enters the RF field, the coupling is disturbed, resulting in a change of signal monitored by the receiver, which then generates an alarm.

b. Two basic types of ported coax sensors are available: pulse and continuous wave.

(1) The pulse type transmits a pulse of RF energy down one cable and monitors the received signal on the other. The cables can be up to 10,000 feet in length. The signal processor initiates an alarm when the electromagnetic field created by the pulse is disturbed and identifies the approximate location of the disturbance.

(2) Continuous wave sensors apply continuous RF energy to one cable. The signal received on the other cable is monitored for electromagnetic field disturbances that indicate the presence of an intruder. Cable lengths are limited to 300–500 feet.

c. Cross section of the detection pattern is somewhat elliptical in shape. An intruder can be detected both above and, to some extent, below the ground. The pattern typically extends 2 feet to 4 feet above the ground and can be 5 feet to 13 feet wide, depending on cable spacing and soil composition. Figure 5–6 represents a typical cross-section of a detection pattern created by a ported cable sensor.

d. Sensor performance depends to a great extent on properties of the medium surrounding the cables. Velocity and attenuation of the RF wave that propagates along the cables and coupling between the cables are a function of the dielectric constant of the soil and its conductivity, which, in turn, depend on its moisture content. For example, the velocity is greater and the attenuation less for cables buried in dry, low-loss soil than in wet, conductive soil. Freeze/thaw cycles in the soil also affect sensor performance. When wet soil freezes, the wave velocity and cable coupling increase and the attenuation decreases, resulting in greater detection sensitivity. Seasonal sensitivity adjustments may be necessary to compensate for changing ground conditions.

e. Although usually buried in soil, ported cables can also be used with asphalt and concrete. If the asphalt or concrete pavement area is relatively small and only a few inches thick, such as a pedestrian pavement crossing the perimeter, the ported cables can be routed beneath the pavement. However, for the large and deep pavements, slots must be cut into the asphalt or concrete to accept the cable.

f. A portable ported coax sensor is available that can be rapidly deployed and removed. The cables are placed on the surface of the ground rather than buried. This sensor is useful for temporary perimeter detection coverage for small areas or objects (vehicles or aircraft, for example).

5–4. Line-of-Sight Sensors

Line-of-sight sensors, which are mounted above ground, generate a beam of energy and detect changes in the received energy that an intruder causes by penetrating the beam. Each sensor consists of a transmitter and receiver and can be in a monostatic or bistatic configuration. For effective detection, the terrain within the detection zone must be flat and free of obstacles and vegetation.

a. Microwave sensors. Microwave intrusion detection sensors are categorized as bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located-at opposite ends of the microwave link, whereas monostatic sensors use the same antenna, or nearly coincident antennas, for the transmitter and receiver.

(1) A bistatic system uses a transmitter and a receiver that are typically separated by 100–1,200 feet and that are within direct line-of-sight with each other. The signal picked up by the receiver is the vector sum of the directly transmitted signal and signals that are reflected from the ground and nearby structures. Detection occurs when an object (intruder) moving within the beam pattern causes a change in net vector summation of the received signals, resulting in variations of signal strength.

(*a*) The same frequency bands allocated by the Federal Communication Commission for interior microwave sensors are also used for exterior sensors. Because high-frequency microwave beams are more directive than low-frequency beams, and the beam pattern is less affected by blowing grass in the area between the transmitter and receiver, most exterior sensors operate at the next to highest allowable frequency, 10,525 MHz.

(*b*) The shape of the microwave beam and maximum separation between transmitter and receiver are functions of antenna size and configuration. Various antenna configurations are available, including parabolic dish arrays, strip-line arrays, and slotted arrays. The parabolic antenna uses a microwave feed assembly located at the focal point of a metallic parabolic reflector. A conical beam pattern is produced (see fig 5–7). A strip-line antenna configuration produces a nonsymmetrical beam that is higher than it is wide. The slotted antenna array produces a beam that is wider than it is high. Larger antenna configurations generally produce a narrower beam pattern.

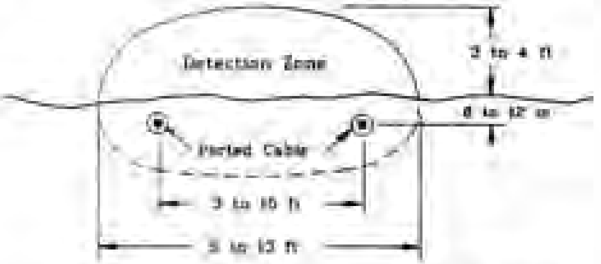


Figure 5–6. Typical Ported Cable Detection Pattern.

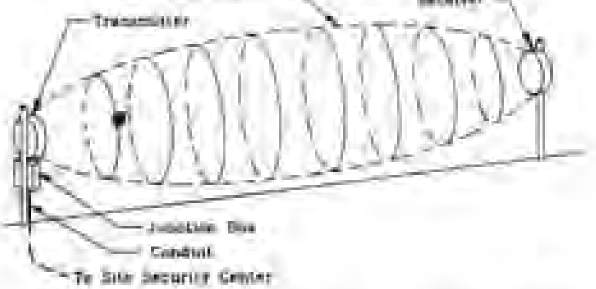


Figure 5–7. Typical Bistatic Microwave Beam Pattern.

(2) Monostatic microwave sensors use the same antenna, or virtually coincident antenna arrays, for the transmitter and receiver, which are usually combined into a single package. Two types of monostatic sensors are available. Amplitude-modulated sensors detect changes in net vector summation of reflected signals, similar to bistatic sensors. Frequency-modulated sensors operate on the Doppler principle, similar to interior microwave sensors. The detection pattern is typically shaped like a tear drop (see fig 5–8). The length, width, and height of the pattern is determined by the antenna array. Monostatic sensors can provide volumetric coverage of localized areas, such as corners or around the base of critical equipment.

b. Infrared sensors. These sensors are available in both active and passive models. An active sensor generates one or more infrared beams, which generate an alarm when interrupted. A passive sensor detects changes in thermal (infrared) radiation from objects located within its field of view. Because only active exterior infrared sensors are currently used at Army facilities, passive exterior sensors will not be addressed in this manual.

(1) Active sensors consist of transmitter/receiver pairs. The transmitter contains an infrared light source, such as a gallium arsenide LED, that generates an infrared beam. The light source is usually modulated to reduce the sensor's susceptibility to unwanted alarms resulting from sunlight or other infrared light sources. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

(2) Active sensors can be single- or multiple-beam systems. Because single-beam sensors can be easily bypassed, multiple-beam systems are generally used in perimeter applications. These are two basic types of multiple-beam configurations; one type uses all transmitters on one post and all receivers on the other post; the second type uses one transmitter and several receivers on each post. Both types are illustrated in figure 5–9.

(3) The spacing between transmitters and receivers can be as great as 1,000 feet when operation is under good weather conditions. However, conditions such as heavy rain, fog, snow, or blowing dust particles attenuate the infrared energy, reducing the effective range to 100 to 200 feet or less.

5–5. Video Motion Sensors

A video motion sensor generates an alarm whenever an intruder enters a selected portion of a CCTV camera's field of view. The sensor processers and compares successive images from the camera and generates an alarm if differences between the images satisfy predefined criteria.

a. There are two categories of video motion detectors: analog and digital. Analog detectors generate an alarm in response to changes in picture contrast. Digital devices convert selected portions of the analog video signal into digital data, which are compared with data converted previously; if differences exceed preset limits, an alarm is generated.

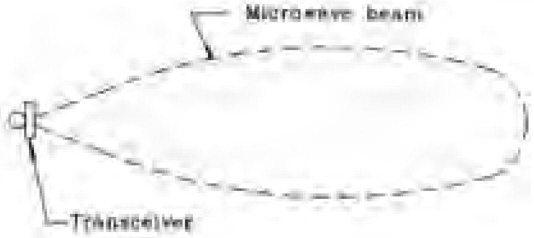


Figure 5–8. Typical Monostatic Microwave Sensor Detection Pattern.

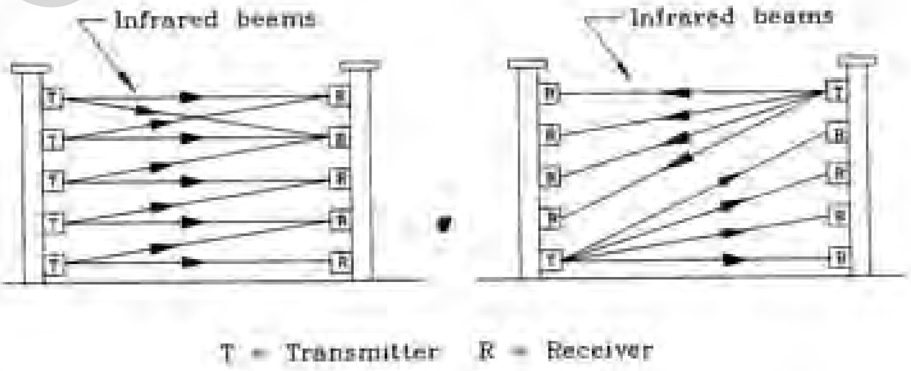


Figure 5–9. Typical Infrared Sensor Beam Patterns.

b. The signal processor usually provides an adjustable window that can be positioned anywhere on the video image. Available adjustments permit changing horizontal and vertical window size, window position, and window sensitivity. More sophisticated units provide several adjustable windows, which can be individually sized and positioned. Multiple windows permit concentrating on several specific areas of an image while ignoring others. For example, in a scene that contains several critical assets and multiple sources of nuisance alarms, such as large bushes or trees, the sensor can be adjusted to monitor only the assets and ignore the areas that contain the nuisance alarm sources.

c. Use of video motion detection systems for exterior applications has been limited, primarily because of difficulties with uncontrolled exterior environments. Lighting variations caused by cloud movement and shadows of slow moving objects, birds and animals moving within the camera field of view, camera motion and moving vegetation during windy conditions, and severe weather conditions have traditionally caused a multitude of unwanted alarms in this type of system. Systems using more advanced signal processing algorithms have improved motion detection capability and nuisance alarm rejection but are still subject to high unwanted alarm rates under certain conditions and, therefore, should be specified with due caution and extreme care.

Section II. DESIGN GUIDELINES

5-6. Basic Design Criteria

Design of a perimeter intrusion detection system involves primarily the selection and layout of exterior sensors that are compatible with the physical and operational characteristics of a specific site. Important factors to consider during the selection process include physical and environmental conditions at the site, sensor performance, and overall cost of the system. Refer to TM 5-853-1 and TM 5-853-2 for additional guidance on the requirements for and placement of exterior sensor systems. Since exterior barriers provide very little delay, exterior sensor systems generally do not provide a significant increase in the available response time.

a. Physical and environmental considerations. These are often the determining factor in selection of exterior sensors. The site's characteristics can significantly affect operational performance of a sensor, both in terms of probability of detection and susceptibility to nuisance alarms. Exterior sensors that are most compatible with the site environment should be chosen.

(1) Weather and climatic conditions at a specific site can significantly influence selection of a sensor. For example, infrared detectors are not very effective in heavy rain, fog, dust, or snow. Deep snow can affect detection patterns and performance of both infrared and microwave sensors. High winds can cause numerous false alarms in fence-mounted sensors. Electrical storms can cause alarms in many types of sensors, and damage equipment as well.

(2) Vegetation can be a significant cause of nuisance alarms. Tall grass or weeds can disturb the energy pattern of microwave and infrared sensors. Vegetation growing near electric field sensors and capacitance sensors can cause nuisance alarms. Large weeds or bushes rubbing against a fence can produce nuisance alarms from fence-mounted sensors. Large trees and bushes moving within the field of view of video motion sensors can cause nuisance or environmental alarms. A clear area must be established for exterior sensors, void of vegetation or containing vegetation of carefully controlled growth.

(3) Topographic features are extremely important. Ideally, perimeter terrain should be flat, although gently sloping terrain is acceptable. Irregular terrain with steep slopes may preclude use of line-of-sight sensors and make CCTV assessment difficult as well. Gullies and ditches crossing the perimeter represent a vulnerability to line-of-sight sensors and may be a source of false alarms (from flowing water) for buried line sensors. Buried metal objects, such as underground utilities, and water flowing through underground culverts can affect performance of buried line sensors. Large culverts can provide an intruder with a route of entry or exit across the perimeter without causing alarm. Likewise, overhead power and communication lines may permit an intruder to bridge the perimeter without causing an alarm.

(4) Large animals, such as cows, horses, and deer, can cause nuisance alarms in both above ground and buried sensors. Sensors sensitive enough to detect a crawling or rolling intruder are susceptible to nuisance alarms from small animals, such as rabbits, squirrels, cats, and dogs. To minimize interference from animals, a dual chain-link fence configuration may be established

around the site perimeter with the sensors installed between the fences.

b. Sensor performance. Exterior sensors must have a high probability of detection for all types of intrusion and have a low unwanted alarm rate for all expected environmental and site conditions. Unfortunately, no single exterior sensor presently available meets both these criteria. All are limited in their detection capability, and all have high nuisance and environmental alarm rates under certain environmental conditions. Table 5-1 provides estimates of probability of detection for various types of intrusion. Table 5-2 lists relative susceptibility of various types of sensors to nuisance and environmental alarms.

c. Economic considerations. Exterior sensor costs are usually given in cost per linear foot per detection zone (typically 300 feet). These costs include both equipment and installation. Fence-mounted sensors, such as strain sensitive cable, electromechanical, and mechanical, are generally less costly than stand-alone and buried-line sensors. Installation costs can vary significantly, depending on the type of sensor. Table 5-3 provides a comparison of relative costs for procuring and installing various types of exterior sensor systems. More detailed cost estimates can be found in agency documentation. It should be remembered that the sensor system cost is only a portion of the total cost for a perimeter IDS. Additional costs include those for fencing, site preparation, CCTV assessment, and perimeter lighting.

5-7. Perimeter Layout and Zoning

The perimeter of a protected area is usually defined by an enclosing wall or fence or natural barrier, such as water.

a. For exterior sensors to be effective, the perimeter around which they are to be deployed must be precisely defined. In most applications, a dual chain-link fence configuration will be established around the perimeter. Typically, fences should be between 30 and 50 feet apart; as the distance increases, it is harder for an intruder to bridge the fences. If fence separation is less than 30 feet, some microwave and ported coax sensors cannot be used. The area between fences, called the con-

Table 5-1. Estimate of Probability of Detection by Exterior Sensors.

	Intruder Technique											
Type of Sensor	Slow walk	Walking	Running	Crawling	Rolling	Jumping	Tunneling	Trenching	Bridging	Cutting	Climbing	Lifting
Fence mounted	N/A	N/A	N/A	N/A	N/A	VH	VL	L	VL	M-H	H	M-H
Taut wire	N/A	N/A	N/A	N/A	N/A	VH	VL	VL	VL	H	H	H
Electric field	VH	VH	VH	H	VH	VH	VL	L	L	N/A	N/A	N/A
Capacitance	VH	VH	VH	H	H	VH	VL	L	L	N/A	N/A	N/A
Ported cable	H	VH	VH	VH	VH	H	M	VH	L	N/A	N/A	N/A
Seismic	H	VH	H	M	M	M	L	M	L	N/A	N/A	N/A
Seismic/magnetic	H	VH	H	M	M	M	L	M	L	N/A	N/A	N/A
Microwave	H	VH	H	M-H	M-H	M-H	VL	L-M	L	N/A	N/A	N/A
Infrared	VH	VH	VH	M-H	M-H	H	VL	L	VL	N/A	N/A	N/A
Video motion	H	VH	VH	H	H	H	VL	L-M	M	N/A	N/A	N/A

VL - very low, L - low, M - medium, H - high,
VH - very high, N/A - not applicable

Table 5-2. Relative Susceptibility of Exterior Sensors to False Alarms.

	Alarm Source											
Type of Sensor	Wind	Rain	Standing water/runoff	Snow	Fog	Small animals	Large animals	Small birds	Large birds	Lightning	Overhead power lines	Buried power lines
Fence mounted	H	M	L	L	VL	L	M	L	L	L	VL	VL
Taut wire	VL	VL	VL	VL	VL	VL	L	VL	VL	VL	VL	VL
Electric field	M	L-H	VL	M	VL	M	VH	L	M	M	L	VL
Capacitance	M	M	VL	M	VL	M	VH	L	M	M	L	VL
Ported cable	VL	M	H	L	VL	VL	M	VL	VL	M	VL	L
Seismic	M	L	L	L	VL	L	VH	VL	VL	L	L	M
Seismic/magnetic	M	L	L	L	VL	L	VH	VL	VL	H	M	H
Microwave	L	L	M-H	L-M	L	M-H	VH	VL	M	L-M	L	VL
Infrared	L	L	L	M	M	M	VH	L	M	L	VL	VL
Video motion	M	L	L	L	M-H	L	VH	VL	M	L	L	VL

VL - very low, L - low, M - medium, H - high, VH - very high

Table 5-3 Exterior IDS Sensor Cost Comparison

Type of Sensor	*Equipment*	*Installation*	*Maintenance*
Fence mounted	L	L	L
Taut wire	H	H	M
Electric field	H	M	M
Capacitance	M	L	M
Ported cable	H	M	M
Seismic	M	M	L
Seismic/magnetic	H	M	L
Microwave	M	M	L
Infrared	M	L	M
Video motion	M	L	M

L—low, M—medium, H—high

trolled area or isolation zone, may need to be cleared of vegetation and graded, depending on the type of sensor used. Proper drainage is required to preclude standing water and to prevent formation of gullies caused by running water after a heavy rain or melting snow. A clear area is required inside and outside the controlled area. This clear area enhances routine observation, as well as sensor alarm assessment, and minimizes protective cover available to a would-be intruder.

b. After the perimeter has been defined, the next step is to divide it into specific detection zones. The length of each detection zone is determined by evaluating the contour, existing terrain, and operational activities along the perimeter. Detection zones should be long and straight to minimize the number of sensors or cameras necessary and to aid guard assessment if cameras are not used. It may be more economical to straighten an existing fence line than to create numerous detection zones in accommodating a crooked fenceline. If the perimeter is hilly and line-of-sight sensors and/or CCTV assessment are used, the length of individual detection zones will be commensurate with sensor limitations. Entry points for personnel and vehicles must be configured as independent zones. This enables deactivation of the sensors in these zones, that is, placing them in the "access" mode during customary working hours (assuming the entry points are manned), without having to deactivate adjacent areas.

c. The specific length of individual zones can vary around the perimeter. Although specific manufacturers may advertise maximum zone lengths exceeding 1,000 feet, it is not practical to exceed a zone length of 300 feet. If the zone is longer, it will be difficult for an operator using CCTV assessment, or for the response force, to identify the location of an intrusion or the cause of a false alarm.

d. When establishing zones using multiple sensors, the designer should, if at all possible, establish coincident zones, where the length and location of each individual sensor will be identical for all sensors within a given zone. If an alarm occurs in a specific zone, the operator can readily determine the approximate location of the alarm by referring to a map of the perimeter. This also minimizes the number of CCTV cameras required for assessment and simplifies the interface between the alarm annunciation system and the CCTV switching system.

5-8. Fence Sensor Design

a. Fence-mounted sensors. Of all exterior sensors, fence-mounted are least costly and easiest to install. They are attached directly to an existing fence and follow the fence contour. Additional installation measures are not required for changes in ground contour, corners, or offsets in the fence.

(1) To make these sensors effective, the fence fabric must be uniformly tensioned (minimum horizontal tension 1,000 lb), fence posts well-anchored, and caps firmly mounted by welding or through-bolts. Vibrations induced by an intruder attempting to lift, cut, or climb the fence are quickly attenuated by a loose fence structure. All fabric connections must be with twisted wire; hog rings will not be used. As a general rule, if a force of 30 pounds is applied at a right angle to the fabric at the center of a panel, it should not deflect more then 2 inches and should return to its original position when released. Fence posts should not deflect more than one-half inch at the top when a force of 50 pounds is applied at a right angle to the post.

(2) These sensors are vulnerable to tunneling under or bridging over the fence. The tunneling threat can be reduced by attaching the fence fabric to asphalt or concrete sills buried in the ground. The bridging threat can be reduced by increasing height of the fence or by mounting barbed wire or rolls of barbed tape on outriggers attached to the top of the fence.

(3) Fence-mounted sensors are susceptible to wind-induced vibration resulting from loose objects striking the fence. Outriggers, barbed wire, and gates must be well anchored so that they do not rattle during windy conditions. Because rolls of barbed tape mounted on the fence can generate numerous unwanted alarms during windy conditions, it is recommended that barbed tape not be used on sensored fences. All fence signs should be removed or fastened so that they will not rattle. All brush and tree branches must be cut or removed, so they do not overhang or rub against the fence.

(4) Nuisance alarms can also be generated by large animals (dogs, deer, and cattle) or by a passerby bumping against the fence. With a double fence configuration, fence-mounted sensors should not be mounted on the outer fence unless required by regulations.

(5) When the fence-mounted sensor is divided into specific detection zones, sufficient overlap should be provided between adjacent zones to ensure detection of an intruder trying to penetrate the fence at the junction between two zones. It is relatively easy to provide overlap of fence-mounted sensors. Usually, the last sensor in one zone is mounted above or below the first sensor in the next zone. Figure 5-10 illustrates how strain-sensitive cable in two adjacent zones should be overlapped.

(6) The use of plastic-coated fence fabric reduces the sensitivity of fence-mounted sensors to climb-over attempts. Gates and fence corners may use larger posts or include diagonal and/or horizontal stiffeners for added strength. Consequently, the fence fabric in these areas may be quite rigid, which also reduces the sensitivity of fence-mounted sensors to climb-over attempts. Additional sensors should be used in these areas to ensure that the entire fence is uniformly sensitive

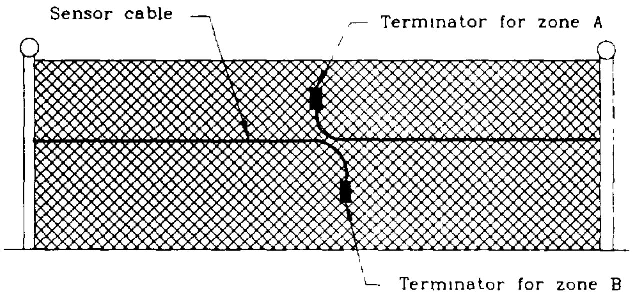


Figure 5-10 Overlap of Fence-Mounted Sensor

to all penetration attempts. Figure 5-11 illustrates how strain-sensitive cable can be looped to increase the sensitivity around the area of a corner post.

b. Taut wire sensors. Taut wire sensors are least susceptible to false alarms of all the exterior sensors. However, they are costly and difficult to install.

(1) Taut wire sensors can be free-standing or attached to an existing chain-link fence or structure. If the sensor is to be attached to an existing fence, the posts must be well anchored and large enough to withstand the tension of the taut wires. This is particularly true for posts located at corners and at ends of the fence, such as at gates.

(2) These sensors can accommodate limited changes in terrain elevation or direction. Generally, the change in that portion of a sensor section on each side of its sensor post should not exceed 15 degrees.

(3) Like all fence sensors, taut wire sensors are vulnerable to tunneling and bridging. The use of a buried sill will reduce the tunneling threat.

c. Electric field sensors. Because of their ability to accommodate turns, these sensors can operate over irregular or hilly terrain and in almost any perimeter configuration. This can be a major consideration in sites where grading is impossible or impractical.

(1) Orientation of the electric field sensor is not critical as long as the sense and field wires are relatively parallel. The sensor can be installed along the ground, vertically on the side of a building, or along the top of a roof. The sensor can be free-standing or attached to an existing fence.

(2) Free-standing sensors are relatively immune to false alarms caused by the wind. However, if the sensor is attached to an existing fence, it is good practice to ensure that the fabric is tight. If not, relative motion between fabric and sense wires (caused by the wind) can generate low frequency signals similar to those of an intruder, resulting in unwanted alarms.

(3) When the sensor is installed along the ground, the vegetation must be cleared or kept short. Grass or weeds close to or coming in contact with the sense wires will usually result in nuisance alarms.

(4) The sensor wires act as antennas; consequently, the sensor is subject to alarms from external electrical interference, such as from high voltage substations and lighting. Depending on the sensitivity adjustment, birds, small animals, and heavy rain or snow can cause unwanted alarms.

(5) The electric field sensor will not work as specified unless it is properly grounded. Equipment must be grounded as recommended by the manufacturer. It is also essential that nearby metal objects, such as a chain link fence, be properly grounded. Installation on a vinyl-coated fence is not recommended because of the lack of a continuous ground reference plane.

5-9. Buried Line Sensor Design

Ported coax sensors can be used to provide intrusion detection around a jagged perimeter with an irregular terrain. An advantage of this sensor, as with most buried sensors, is that precise location of the detection pattern is concealed.

a. Performance of ported cable sensors is affected by electrical conductivity of the soil. The designer will ensure that accurate soil conductivity test data are available from the survey or will perform the necessary testing to determine the conductivity. These sensors perform best with soil conductivities of less than 200 millimho/meter. For

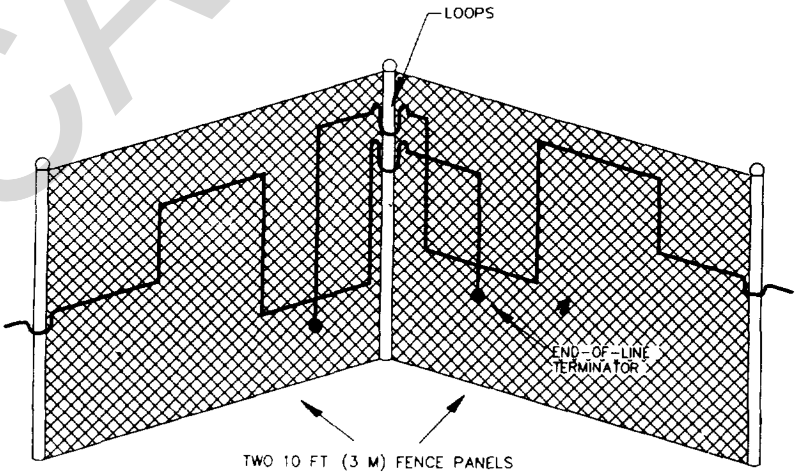


Figure 5-11 Use of Strain-Sensitive Cable Around Corners

sites with higher conductivities, it may be necessary to replace existing soil with a soil having a lower conductivity, such as sand. The electrical conductivity of the soil also changes with ground freeze/thaw cycles. Frozen soil exhibits a lower conductivity, resulting in a higher sensor sensitivity. For this reason, it is necessary to make seasonal hardware adjustments to compensate for sensitivity changes.

b. Ported cable sensors are sensitive to changes in dielectric properties and conductivity in the area around the cables. Hence, they are sensitive to motion of water caused by heavy rainfall, water runoff, and wind disturbance of standing water over the cables. To minimize water problems, the perimeter should be so graded that water will drain away from the sensor bed.

c. The designer must survey the perimeter with a magnetometer to ensure that the sensor bed does not contain metallic objects in close proximity that may affect sensor performance. When sensor cables are routed along or between chain-link fences, the cables should be installed at least 6 to 10 feet from the fence, to avoid field distortions and to reduce potential alarms from motion of the fence fabric during windy conditions. The cables should not be routed under chain-link fences or over metallic objects. If the cables must be routed under a fence, the section of chain-link fabric above the cables should be replaced by a nonmetallic material. Also, if metallic pipes, cables, or culverts containing running water are to be routed under the sensors, they should be buried at least 3 feet below the sensor cable.

d. Ported coax sensors can be used in both soil and paved (asphalt or concrete) areas.

(1) When used in soil, the cables are usually buried at a nominal depth of 9 inches. The cable trench is partially filled with a layer of sand, approximately 4 inches deep, to cushion the cable. The trench is backfilled with native soil to provide a measure of erosion control. Burial depth and cable separation should be consistent, in order to achieve uniform sensor response. Sharp turns at corners must be avoided, because the electromagnetic field may extend farther from the cable than desired.

(2) For thin pavements, 2 inches or less, the sensor cables should be buried in soil under the pavement. For thicker pavements, cables should be embedded in grooves or slots, cut approximately 2 inches deep, in the pavement. The grooves should be filled with nonshrinking filler. The filler not only protects the cable, it provides a closer coupling to the pavement resulting in higher detection sensitivity. Sensor turns in locations subject to heavy traffic or wheel loads should be avoided.

(3) Transitions between burial mediums, such as soil to asphalt or asphalt to concrete, should be minimized. Changes in detection sensitivity will also occur between different burial mediums. The sensor must be calibrated to ensure that a standard intruder moving within the specified velocity range will be detected at all locations along the sensor cable.

e. With pulsed sensors, detection zones are established electronically. There are no problems with interference between adjacent zones or with zone overlap. Continuous wave sensors use multiple transceivers and cable sets. Adjacent zones should be operated at different frequencies to avoid interference. To ensure that an intruder cannot penetrate the perimeter at the junction between the zones, the cables in one zone should be slightly offset and routed parallel to the cables in the next zone. Figure 5-12 illustrates a method of overlapping ported cable sensors.

5-10. Line-of-Sight Sensor Design

a. Microwave sensors. These sensors can provide perimeter intrusion detection for sites that are reasonably level and have boundaries straight enough to accommodate detection zone lengths of several hundred feet.

(1) The terrain between transmitter and receiver should be relatively flat, with no more than a plus or minus 3-inch deviation from a plane between the bases of transmitter and receiver. The sensor bed must extend a minimum of 7 feet on each side of the beam centerline or the maximum mid-range beam width of a specific sensor, whichever is greater. The surface must be graded to drain water away from the sensor bed, since ripples in standing water are potential sources of nuisance and environmental alarms.

(2) The surface of the sensor bed can be dirt, sand, gravel, asphalt, concrete, grass, or a combination of these. If grass is used, its height should

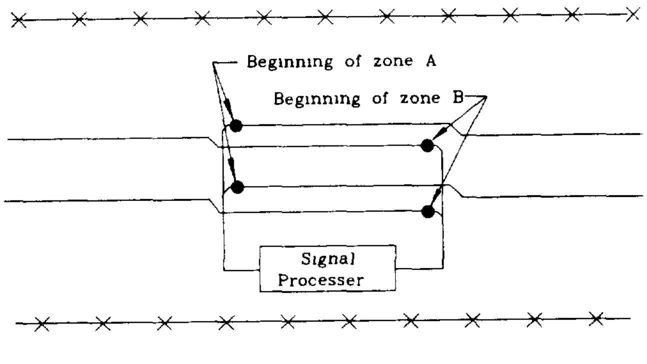


Figure 5-12 Overlap of Ported Cable Sensors.

not be allowed to exceed 4 inches. Wind-induced movement of grass or weeds can impair the performance of the sensors, as well as cause nuisance and environmental alarms.

(3) When microwave sensors are installed parallel to a chain-link fence, an adequate distance should be maintained between beam centerline and fence fabric, since movement of fabric during windy conditions is a potential cause of unwanted alarms. A minimum distance of 10 feet will be maintained between the beam centerline and the fence.

(4) Microwave sensors can operate through chain-link fences if the beam centerline is nearly perpendicular to the fence. This feature is useful at portals in the perimeter, where chain-link fences may cross the intrusion detection zone in a direction perpendicular to perimeter fencing.

(5) An accumulation of several inches of snow will not usually affect performance of these sensors. However, if accumulations are 6 inches or greater, an intruder can crawl through the snow with very little probability of being detected. Where snow accumulation is a problem, provision must be made by the using activity to ensure adequate removal as soon as possible after a snow fall.

(6) By far, the most difficult problem with bistatic microwave sensors is to provide adequate overlap between adjacent zones.

(*a*) Typically, microwave transmitters and receivers are mounted on a post 2 to 3 feet above ground. The area directly beneath the units is not within the detection pattern. This area, known as the dead zone, is illustrated in figure 5-13. Length of the dead zone may vary from 10 to 50 feet, depending on the type and height of the antenna. Although the figure shows the dead zone beneath the unit, it also extends above the unit. To protect against intruder penetration, the dead zone must be within the detection pattern of the adjacent zone. Hence, adjacent zones must be overlapped. The overlap must be adequate to detect a low crawling intruder midway between overlapping zones and at beam intersections in corners. Figure 5-14 shows examples of corner overlap and parallel overlap. In this figure, the distance "d" represents the length of the dead zone.

(*b*) In addition to providing protection against an intruder crawling through or jumping over the microwave units, the overlap should also prevent the intruder from crossing behind and between units. Two techniques are commonly used to lay out microwave zones. In one, transmitter and receiver units are installed near the center of the controlled area; the microwave beams are parallel to each other in the overlap region. The offset between centerlines of the two beams should be less than that required for an intruder to walk between the beams without being detected. The second layout is known as the basketweave configuration. In this case, transmitter and receiver units are located on the sides of the clear zone, which is useful when it is necessary to drive a large vehicle, such as a snow plow, through the center of the controlled area. With this technique, the microwave beams of adjacent zones crisscross, preventing an intruder from passing between them. Figure 5-15 illustrates both methods. When using the basketweave configuration, the microwave receivers should be located on the protected, or inner side, of the perimeter sensors. This provides additional tamper protection for the signal processing and alarm circuitry, which is usually housed in the receiver enclosure.

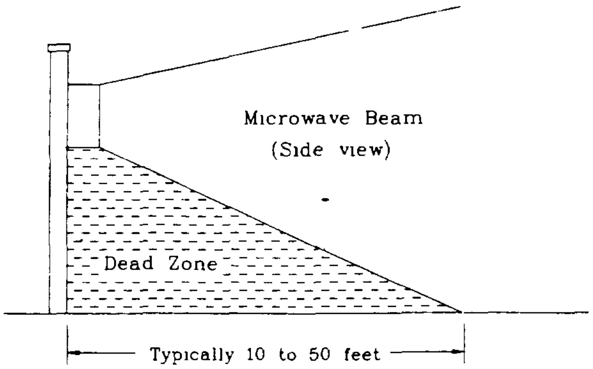
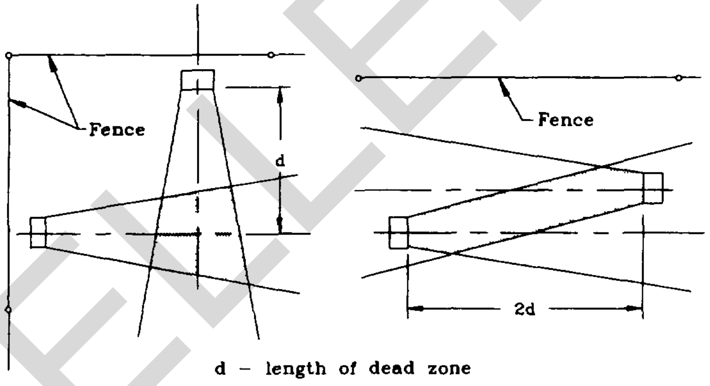


Figure 5-13 Microwave Dead Zone.

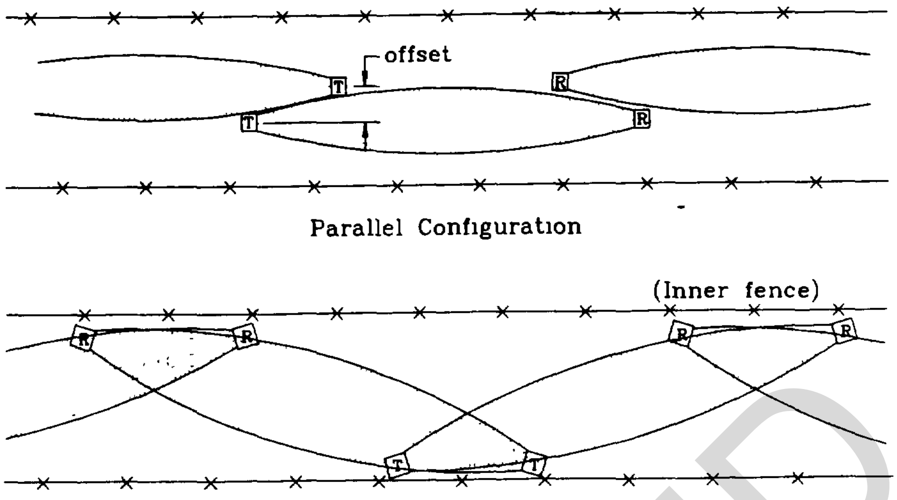


Corner Overlap

Parallel Overlap

Figure 5-14 Overlap of Microwave Zones.

(*c*) As mentioned previously, length of the dead zone is a function of antenna height. Lower



Parallel Configuration

Basketweave Configuration

Figure 5-15. Microwave Layout Configurations.

ing the antenna decreases the length of the dead zone. However, height of the overall detection zone is also decreased. Use of a stacked microwave configuration, such as two transmitters or receivers mounted on the same post, allows for a shorter dead zone, as well as a higher detection zone. This method is illustrated in figure 5-16.

b. Infrared sensors. Like bistatic microwave sensors, infrared sensors can be used to provide intrusion detection for perimeters that are reasonably straight and level.

(1) The detection zone of this sensor is basically a vertical plane several feet high by several inches wide. Transmitters and receivers can be stacked together to form a vertical column of sensors of the necessary height. For most applications, the units are stacked from ground level to a height deemed adequate to preclude an intruder from jumping over the beams, usually about 6 feet. Some manufacturers offer sensors that are factory assembled units with a fixed number of transmitters and receivers that cannot be field modified. Others offer modules that can be assembled in the field to meet site-specific applications. Effective width of the vertical detection plane is determined by size of the lenses associated with light transmitters and receivers. Generally, these lenses are 3 to 4 inches in diameter. Because of the narrow width of the detection zone, infrared sensors can usually be installed close to fences or buildings. However, they must not be located near objects that may allow an intruder to jump over the narrow beam.

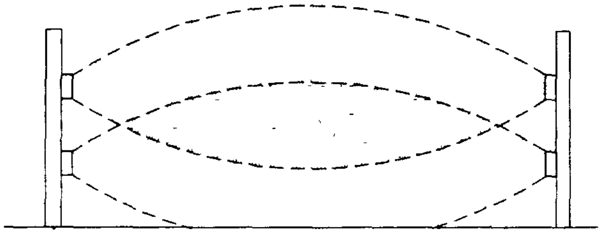


Figure 5-16. Stacked Microwave Configuration.

(2) As with all line-of-sight sensors, the detection zone must be kept clear of objects that block the beams. Vegetation must be removed or its growth controlled. Snow cannot be allowed to accumulate enough to block the bottom beam, which should be low enough, usually about 6 inches above the ground, to detect the crawling intruder.

(3) As with other sensors, adjacent detection zones should be overlapped to prevent intruder penetration at the junction of the zones. If two adjacent columns of sensors are installed in the same enclosure, the top of the enclosure should include a pressure switch or some other method of detecting an intruder trying to climb over the column.

(4) Because of narrow beams, alignment of corresponding transmitters and receivers is critical. The alignment becomes more difficult as the distance between the transmitters and receivers is increased. Any angular movement or deflection of sensor columns can cause misalignment, resulting in nonfunctional or marginally functional sensors. Misalignment can be caused by column movement in the ground, typically from freezing or thawing cycles or from something hitting a column. Movement caused by freezing or thawing must be minimized by installing the column foundation

deep enough to prevent excessive movement. Physical barriers should be installed to prevent lawn mowers, snow removal equipment, or other types of equipment from striking the columns.

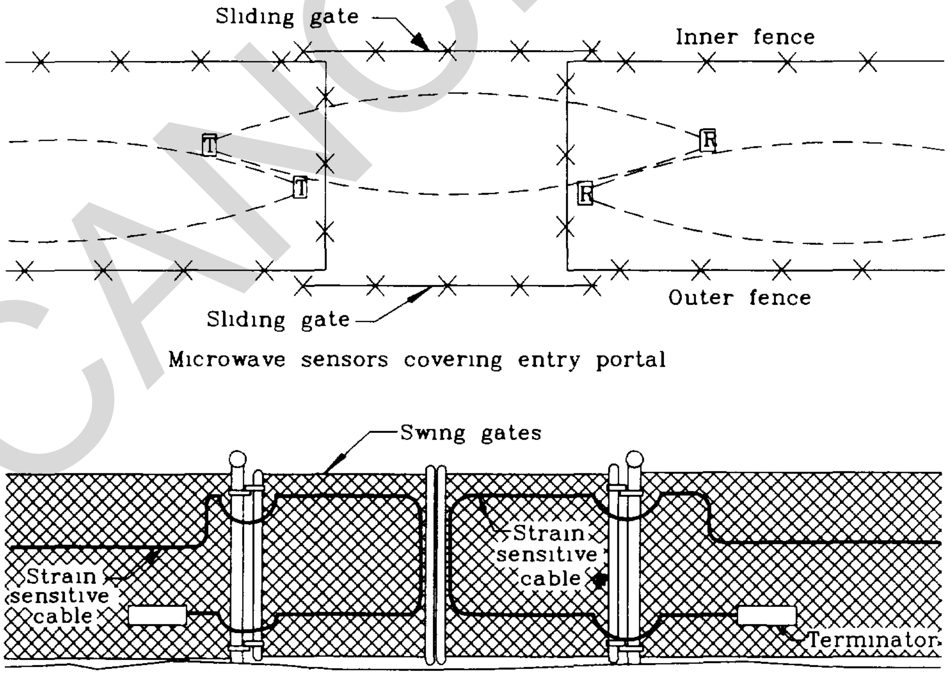
5-11. Other Considerations

Additional factors to be considered during design of a perimeter IDS include providing intrusion detection coverage around obstacles located on the perimeter, providing adequate protection for equipment, using combinations of sensors, and having self-test capability.

a. Perimeter obstacles. Unfortunately, all perimeters usually contain several obstacles that require special consideration. For example, entry portals or sallyports are usually provided for personnel or vehicles to enter and leave the protected area. At some sites, small buildings used for entry control and the Security Center may be located directly on the perimeter boundary. Drainage culverts large enough to permit man-sized passage may cross the perimeter. Overhead electrical power lines or communication lines may provide an intruder with means to bridge the perimeter. Techniques for providing adequate IDS protection for these obstacles are discussed in the following paragraphs.

(1) *Entry portals.* All perimeters with IDS usually have one or more controlled entry points where personnel and vehicles are allowed entry and egress. If there is continuous traffic at these points, IDS may not be required. However, if traffic is intermittent or if the entry point is not manned continuously, IDS is usually required. Sensors selected for the perimeter may or may not be suitable for use at entry points. For example, taut wire sensors and electric field sensors are usually not suitable. However, line-of-sight sensors, such as bistatic microwave or active infrared, adapt easily to these applications. Fence sensors can be used on gates if properly installed to permit opening or closing the gate. Figure 5-17 shows several applications using exterior sensors at perimeter entry points.

(2) *Perimeter buildings.* Small buildings, such as those used for housing guards at entry control points, may form part of the perimeter at a site. To be effective, the perimeter IDS must be continuous over and around the building. The sensors must be configured to detect an intruder trying to climb the walls or use the roof to penetrate the perimeter. Stand-alone fence sensors, such as electric field, capacitance, or taut wire, can be used around upper edges of building walls and on sides of the building. Line-of-sight sensors can be installed on the roof. When microwave sensors are used around the perimeter, metal reflectors mounted on building walls can be used to eliminate the offset problem for zones ending at the walls. To determine how best to configure a sensor



Microwave sensors covering entry portal

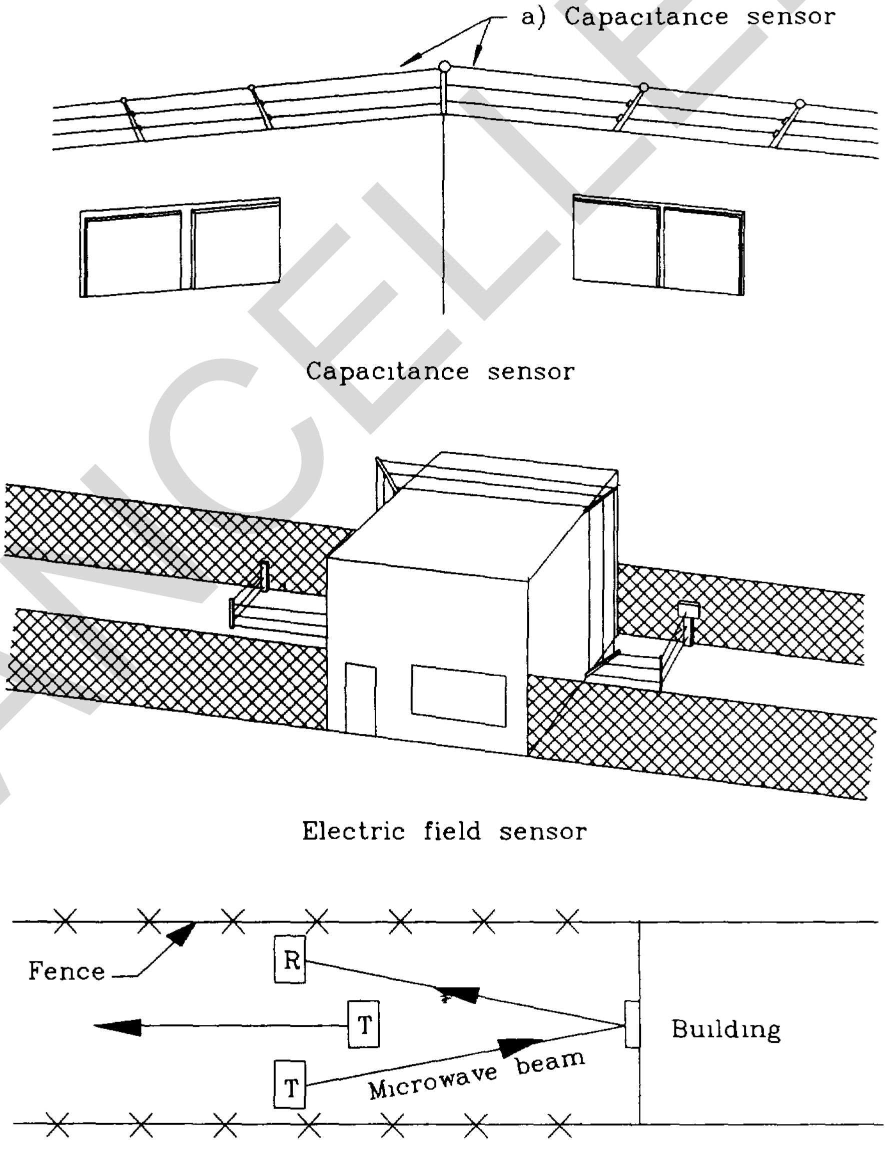
Strain sensitive cable on swinging gates

Figure 5-17 Applications of Exterior Sensors at Perimeter Entry Points

to cover walls and roof of a building, specific sensor installation manuals should be reviewed. Figure 5-18 shows several applications using exterior sensors for intrusion detection around buildings.

(3) *Culverts.* Large culverts or storm sewers can provide an intruder with a path to cross the perimeter without being detected. The most effective protection against this type of entry or exit is to replace large pipes with several smaller pipes, each having a cross section less than 96 square inches. If ported cable sensors are deployed around the perimeter, this method is preferred. Large pipes can also be secured by welding several smaller diameter pipes inside the large pipe or by attaching a bar grill across each end of the pipe. The bar grill can be fabricated with hollow bars, through which a strain-sensitive cable or grid-wire sensor can be installed. A bar grill equipped with strain sensitive cable will initiate an alarm if the bars are cut or an attempt is made to remove the assembly. However, nuisance alarms from debris striking the bars may be a problem. Bar grills equipped with a grid-wire sensor are not sensitive to nuisance striking debris, but the entire assembly must be tamper-protected against removal.

(4) *Overhead lines.* Overhead power lines and communication lines crossing the perimeter can offer an intruder a path to bridge the perimeter IDS. Unfortunately, there is no reliable method of providing effective intrusion detection coverage against overhead line penetration. The most affec-



Capacitance sensor

Electric field sensor

Microwave sensor with reflector

Figure 5-18. Applications of Exterior Sensors Used for Intrusion Detection Around Perimeter Buildings

tive protection is to replace overhead lines with underground lines. A less costly alternative, but also less effective, is to place large barriers, such as aircraft warning balls, on the overhead lines.

b. Equipment protection. All intrusion detection equipment must be protected from tampering, so that its effectiveness cannot be compromised. This can be accomplished by providing tamper-resistant enclosures and by locating equipment within the protected area.

(1) All enclosures, cabinets, boxes, and fittings that have hinged doors or removable covers and that contain IDS circuitry, power supplies, or wiring connections, must be provided with cover-operated tamper switches. These switches must initiate an alarm signal whenever the door or cover is removed. The alarm annunciation system must never allow tamper switches to be placed in the "access" mode.

(2) Additional protection can be provided by installing all sensor-related equipment on the protected side of the perimeter. For example, if a fence is equipped with a fence sensor, the signal processor for the sensor should be installed inside the fence. (Note: When providing perimeter IDS protection for prisons, the area outside of the fence is considered to be the protected area.) When using buried line sensors, signal processors should be located on the protected side of the buried sensors. With line-of-sight sensors, such as bistatic microwave devices, more care must be exercised in laying out equipment. The signal processor and associated alarm circuitry are usually located in the receiver unit; hence, the receiver unit will be located toward the protected side of the clear zone. If it is not possible to design the layout with all receivers on the protected side, it may be necessary to provide an additional sensor to protect the equipment For example, receiver units located in perimeter corners can be protected with monostatic microwave sensors.

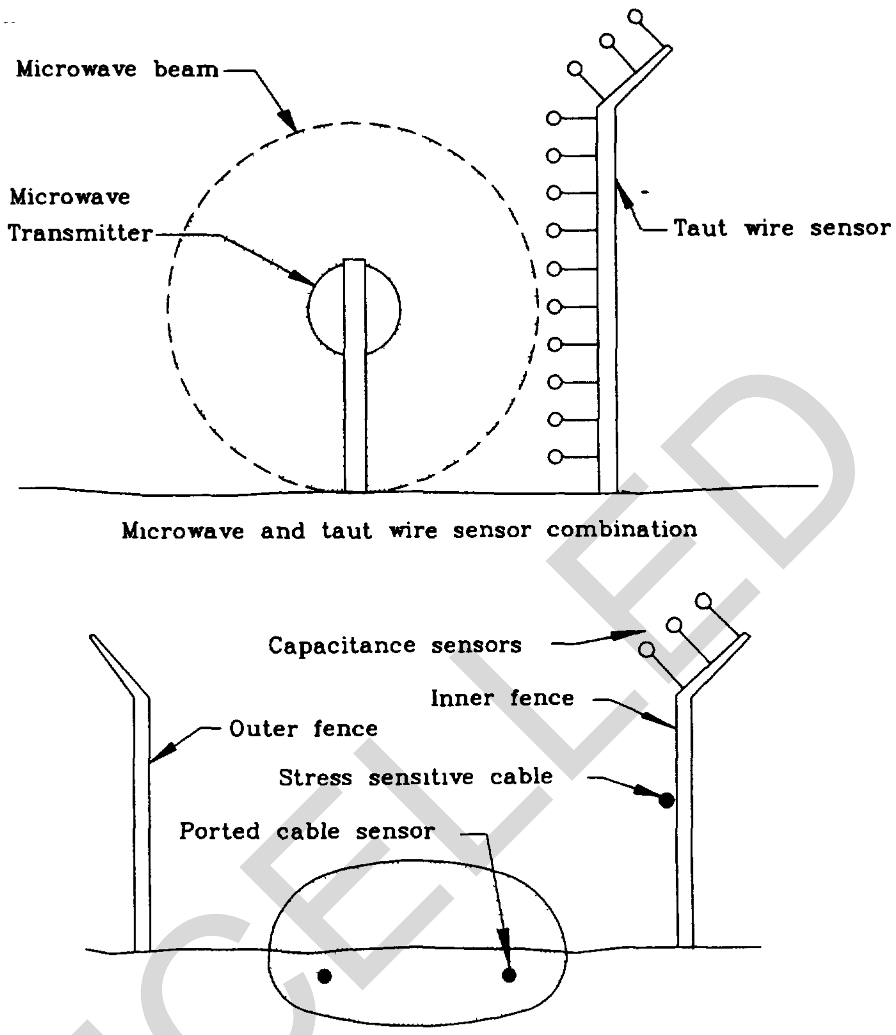
(c) Combinations of sensors. No single exterior intrusion detection sensor available can detect all types of intrusions in a normal outdoor environment. Single sensors can be used in areas that require protection from the casual intruder who climbs fences and walks or runs through an area. Where greater protection is necessary, a combination of two or more diverse sensors must be used to ensure detection of a skilled intruder. Combination choices may include, for example, a fence sensor behind a line-of-sight sensor, a fence sensor and a buried line sensor, or a line-of-sight sensor and a buried line sensor. Sensor combinations will be selected in such a way that the strengths of one sensor compensate for the weaknesses of the others. When two or more sensors are deployed, the sensor outputs may be combined through any of a number of different techniques.

(1) *"OR" combination.* The most common technique for combining sensor outputs is the logical "OR" combination, where the sensor outputs are combined by an "OR" gate, so that an alarm is generated when any sensor is activated. Practically, the "OR" technique is achieved by monitoring each sensor output individually. With this technique, the probability of valid detection is increased; however, the overall nuisance and environmental alarm rate for each detection zone is also increased, because the overall rate is the sum of nuisance and environmental alarm rates of individual sensors. In using the "OR" technique, it is desirable to choose sensors whose detection patterns complement each other. Examples of complementary exterior sensors are shown in figure 5-19.

(2) *"AND" combination.* Sensor outputs can be combined by using a logical "AND" gate. With this arrangement, a valid alarm is generated only when all sensors are actuated. Because a single penetration attempt rarely activates all sensors simultaneously, the "AND" logic must be designed with a time window, so that an alarm is generated if each sensor produces an alarm within a defined time interval. Use of the "AND" combination will significantly reduce the false alarm rate. This is especially true if the sensors do not respond to the same alarm stimuli, such as high wind or other environmental conditions. On the other hand, the probability of detection decreases, because all sensors must be activated within the defined time interval for an alarm to be generated. Also, if the "ANDed" sensors are not completely redundant and overlapped, it may be possible to cross the perimeter completely undetected by first crossing a sensor in one zone, then crossing the second in an adjacent zone or simply waiting for the preset time window to time out before crossing the second sensor. "AND" logic should be used only to solve a problem that cannot be solved with more conventional means.

(3) *Majority logical combination.* When three or more sensors are used, outputs from each sensor can be combined into a majority logical arrangement. For example, an alarm can be generated when any two of three sensors are activated. This reduces vulnerability of "ANDed" sensors, because more than one sensor must be defeated. Combining sensor outputs by using majority logic will also reduce false alarm rates.

d. Self-test capability. As with interior sensors, providing exterior sensors with self-test capability



Microwave and taut wire sensor combination

Ported cable and fence sensor combination

Figure 5-19. Complementary Exterior Sensors.

to verify their operation is a very desirable feature. With some sensors, this feature is fairly easy to implement. For example, with line-of-sight sensors, an intrusion can be simulated by momentarily turning the transmitter off. Ported coax sensors use "test targets" buried adjacent to sensor cables, which, when activated, disrupt the normal electromagnetic field of the sensor. However, implementing the self-test feature on some types of sensors, such as fence sensors, is quite difficult. Rather than simulating actual movement of the fence, an electronic signal simulating fence movement is generated, which is used to verify the operation of the electronic circuitry. When selecting exterior sensors, their self-test capability and the means of implementing it should be carefully examined.

CHAPTER 6

IDS ALARM ANNUNCIATION SYSTEM

Section I. HARDWARE

6-1. IDS Alarm Annunciation

Field device status information from the various intrusion detection sensors must be collected from the field and transmitted to the IDS alarm annunciation system in the Security Center, where it is processed, annunciated, and acted upon by security personnel. The IDS alarm annunciation system may also interface with the CCTV and EECS systems. There are typically two types of IDS configurations available. The simplest configuration, which is suitable for small installations, is the point-to-point configuration. With this configuration, a separate transmission line is routed from the protected area to the Security Center, and is shown in figure 6-1. J-SIIDS is typical of this type of configuration and will not be further discussed in this manual. The second, and more popular type, is a digital multiplexed configuration that allows multiple protected areas to communicate with the Security Center over a common data line. The block diagram of a typical multiplexed IDS alarm annunciation system is shown in figure 6-2.

6-2. IDS Alarm Annunciation Configuration

A block diagram of a typical IDS alarm annunciation system is shown in figure 6-3. As shown in the figure, the central computer is the hub of IDS information flow. The central computer receives and displays alarm and device status information and sends operator control commands to the IDS local processors. It also interfaces with the CCTV and electronic entry control systems. For larger facilities, the management of the DTM communication tasks may be delegated to a separate communication processor so that the central computer can turn its full attention to interpreting the incoming information and updating the control and display devices located at the security console (display, logging, control, and storage devices).

a. Central computer. The central computer may consist of one or more digital computers. Depending on IDS size and speed requirements, the computer may be a micro, mini, or mainframe. To provide a time stamp for IDS events, a real-time clock will be included.

b. Redundant central computers. If the value of IDS protected assets is high, redundant central computers may be required. They will be connected in a peer configuration where each monitors IDS device status independent of the other. However, only one computer (the main computer) is allowed to present information to the console operator and sends commands to the field devices.

c. Failover controller. In a redundant central computer configuration, a failover controller monitors the main computer's operation and, upon a detection failure, transfers control to the redundant computer and informs the console operator that the IDS is operating without a back-up computer. The design should provide that the console operator may command a transfer back to the main computer after the failure has been repaired.

d. Security console I/O bus. The typical security console devices that communicate with the central computer are depicted in the top right and left hand sides of figure 6-3. The devices provide alarm display, logging, control, hardcopy, and archival storage. If these devices are supplied by the vendor of the central computer, there will be I/O compatibility. If the devices are to be supplied by different vendors, the device specifications should each include an I/O bus specification to ensure I/O bus compatibility. To expose their products to the widest possible markets, manufacturers of such equipment provide equipment that conforms with either the EIA RS-232 serial or Centronix parallel interface protocol. It is not uncommon to find I/O bus equipment that is capable of supporting both.

e. Real-time clock. The real-time clock provides a time stamp for IDS events and allows for time synchronization with CCTV and EECS if included. The clock must be settable by the console operator, should include battery backup, and be readable by all systems elements so that system events are properly time correlated. As an example, there will be exact time correlation for an IDS alarm event reported on the alarm printer and the corresponding video scene recorded by the CCTV video processor.

6-3. Data Storage

With computer-based systems, it is necessary to store large amounts of information, such as system software, application programs, data structures, and IDS events such as alarm transactions and status changes. Hence, a large amount of non-

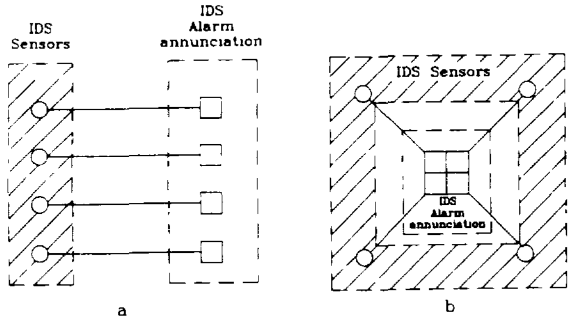


Figure 6-1 Typical Point-to-Point IDS

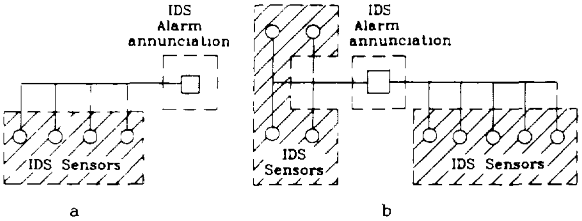


Figure 6-2 Typical Multiplexed IDS.

volatile memory is required. The semiconductor memory provided with a central computer is designed for rapid storage and retrieval, with access times measured in nanoseconds. Because this type of memory is quite costly, more economical means are generally chosen for storing large amounts of data. The most commonly used media for archival storage are magnetic tapes and magnetic disks.

a. Magnetic tape. Approximately 2,400 feet of ½-inch tape can be wound on reels of up to 10.5 inches in diameter, providing a storage capacity of 180 megabytes of data. Small magnetic tape cartridges, approximately 4 inches square, that can store 200 megabytes on ½-inch tape are available for main-frame computers. Quarter-inch cartridges storing up to 60 megabytes are available for small computers. A major limitation of using magnetic tape for mass storage is the intrinsically long access times, typically measured in seconds, required to retrieve selected data. Hence, magnetic tapes are primarily used for backup storage.

b. Hard disks. The large hard disk units provided for mainframe computers generally have provisions for removing and replacing one or more of the platters. However, the smaller "Winchester" units, commonly used on smaller systems, are completely sealed. Hard disks have access times measured in tens of milliseconds and can store several hundred megabytes of data. They are used to store system and application programs, includ-

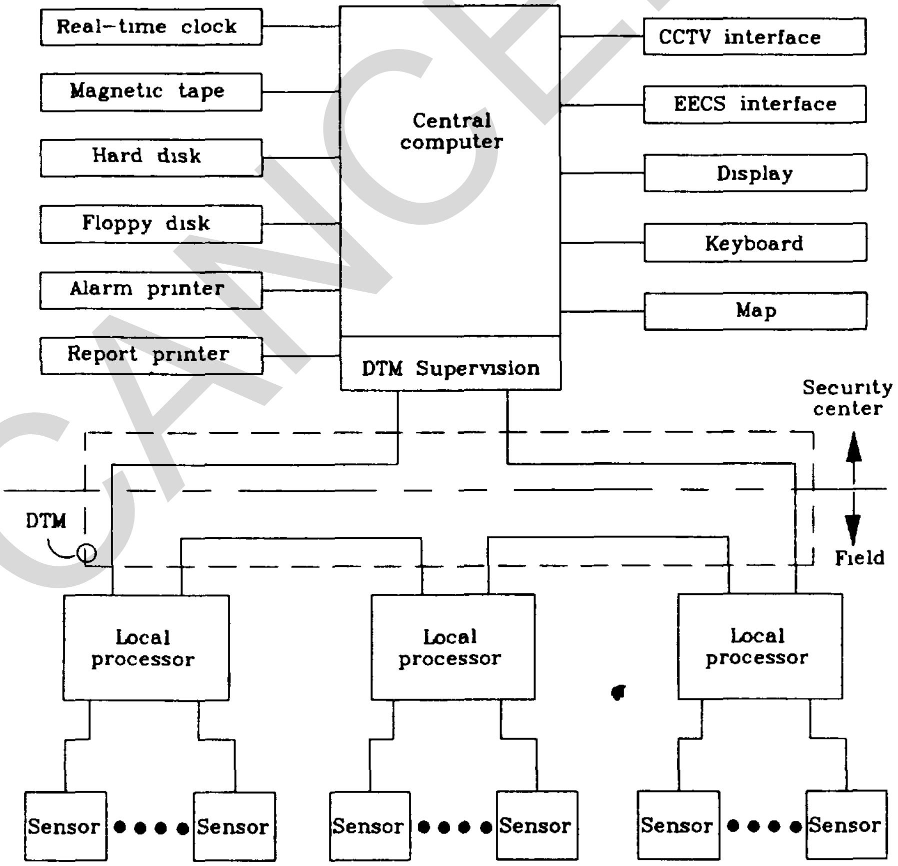


Figure 6-3 Typical IDS Alarm Annunciation System.

ing temporary storage of alarm and operator activity.

c. Floppy disks. Floppy disks are available in 5.25-inch (360-kilobyte or 1.2-megabyte capacity) and 3.5-inch (720 kilobytes or 1.44 megabytes capacity) format. Floppies are used for initial system software and data installation as well as for archival storage of small amounts of system activity.

6–4. Operator Interfaces

The operator interacts with the IDS equipment by means of devices that can be seen, heard, or touched and manipulated. Hence, visual displays and printers can be used to inform the operator of an alarm or equipment status. Audible devices can be used to alert an operator to an alarm or equipment failure. Devices such as push buttons and keyboards permit an operator to acknowledge and reset alarms, as well as change operational parameters.

a. Visual displays. The type of display used to inform the operator visually of the security status of protected areas is determined primarily by the complexity of the system. Status information may be displayed on numeric displays, monitors, or a map display. Each of these display techniques is discussed more fully in the following subparagraphs.

(1) *Alphanumeric displays.* This type of display uses indicator lamps or LEDs to display letters and numerals that provide information relative to the alarm circuit status. This information may include the type of event (alarm, changes in access/secure status, power failure, etc.) and a number that corresponds to the location of the event. Frequently, a set of indicator lights is used in conjunction with the display; the lights indicate the type of event and the display identifies the location. Because all alarm information is processed and displayed through one common set of electronics, this display technique is quite cost effective. Also, the equipment requires only a small amount of physical space. However, if there is an equipment failure, the entire reporting capability will be lost. Another consideration is that only one alarm event can be displayed at any time. In most alphanumeric display systems, concurrent events are processed serially on a first-in, first-out basis. Therefore, a high priority event may not be displayed until after a lower priority event has been acknowledged, assessed, and reset by the operator. Also, it may not be possible to determine if there are multiple events until each event has been acknowledged and reset by the operator.

(2) *Monitors.* Monitors provide great flexibility in the type of alarm information that may be displayed and the format in which it may be displayed. Both text and graphic information can be displayed in a variety of colors. Multiple alarms may be displayed. If alarms are prioritized, higher priority alarms may be highlighted by blinking, by using bold print or reverse video, or by changing colors. To assist the operator in determining the correct response, alarm-specific instructions may be displayed adjacent to the alarm information. However, as with the alphanumeric display, a major disadvantage is that all reporting capability is lost if equipment failure occurs.

(3) *Map displays.* Map displays are used to identify zones of detection on a pictorial representation of the protected area. A map display can be a board-mounted drawing with indicator lights to identify the zones of detection or a computer-generated monitor display. A large map display provides a very quick and convenient way to observe the security status of the entire protected area. If the board is not too cluttered, it may also be used as an annunciator panel by providing additional indicator lights to depict access/secure status. A disadvantage of the board display is the difficulty in modifying the board to accommodate changes in the IDS protection scheme. A computer-generated map display has limited resolution. However, this disadvantage can be overcome by providing multiple displays, each showing a small portion of the protected area. Usually, the correct map can be displayed automatically when an IDS zone goes into alarm. The selection of an appropriate map display depends on:

(*a*) Number of areas being protected.

(*b*) Overall size of the installation.

b. Audible alarm devices. In conjunction with the visual display of an alarm, most IDS alarm annunciation systems can also generate an audible alarm. The audible alarm may be produced by the ringing of a bell or by the generation of a steady or pulsating tone from an electronic device. In any case, the audible alarm serves to attract the operator's attention to the visual alarm display. A silence switch is usually provided to allow the operator to silence the bell or tone before actually resetting the alarm. In computer-based systems, the audible alarm may sometimes be supplemented by a verbal message generated by a digital voice synthesizer.

c. Logging devices. All alarm system activity, such as a change of access/secure status, an alarm event, or a trouble event, should be logged or recorded, as in many cases is required by regulation. Logged information is important not only for security personnel involved in the investigation of an event but also for maintenance personnel checking equipment performance for such causes as false and nuisance alarms. Most microprocessor or computer-driven alarm annunciation systems have provisions for logging information automatically on printer-generated hard copy. Several types of printers are available for information logging, depending on IDS size.

(1) *Strip printer.* The logging requirements of a small IDS may be met by the roll, or strip, printer. It is a small, compact printer, which typically prints on 3.5-inch wide paper. Because of its compact size, only a limited amount of information can be logged. Some printers will print change-of-status information in black and alarm information in red.

(2) *Page printer.* A moderately sized IDS will require a larger printer using 8.5 to 17-inch wide paper. These printers may print one character at a time or an entire line or block of characters at a time. Printers with a printing speed of 150 characters per second, capable of 132 characters per line are typical.

d. Report printer. Most IDS facilities will require a separate report printer for generating reports using information stored by the central computer. This printer will usually be the same type as the logging printer.

e. Operator control. A means is required to transmit information from the operator to the system. The type of controls provided usually depends on the type of display provided.

(1) *Keypads.* A numeric display system will generally be provided with a 12-digit keypad and several function keys such as access, secure, acknowledge, and reset. The keypad enables an operator to key in numeric requests for the status of specific zones.

(2) *Keyboards.* Monitor-based systems are usually provided with a typewriter-type keyboard, which enables an operator to enter more information, using a combination of alphanumeric characters.

f. Enhancement hardware. More sophisticated systems may provide a touch screen monitor through which the operator may enter information by touching selected areas of the monitor screen. Additional devices, such as light pens, joysticks, and trackballs, may also be provided with these systems.

6-5. IDS Field Data Collection

Sensor data are transmitted to the IDS alarm monitor located in the Security Center over the DTM selected. Information received from intrusion detection sensors is binary in nature, meaning it can assume only one of two states, such as a switch being open or closed.

a. Local processors. For binary information, multiplex techniques can be used to minimize the number of data links needed to communicate sensor status to the Security Center. This is accomplished by the use of devices called "local processors" (also referred to as data gathering panels or remote field panels).

(1) Depending on the manufacturer, a local processor may have as few as 4 device inputs or as many as 128. Rather than having a fixed number of inputs, many local processors are expandable. For example, a basic local processor may be provided with eight device inputs, with additional blocks of eight inputs available by means of plug-in modules.

(2) The local processor input circuitry must include line supervision capability. Usually, DC line supervision is supplied as a standard, with more secure techniques available as options. The data communication between the local processor and the alarm monitor must also provide line supervision.

(3) In addition to device input circuitry, local processors can also provide output signals that can be used for such functions as activating sensor remote test features, light control, or activating a deterrent, such as a loud horn.

(4) A local processor can be "dumb" or "smart." A dumb processor contains the basic circuitry necessary to combine a number of sensor inputs into one digital status word. Its function is to transmit this word when queried by the IDS central computer located in the Security Center. A smart local processor contains a microprocessor, solid-state memory, and appropriate software. It has the capability to perform a number of functions locally, such as access/secure mode selection, alarm reset, and device testing. If the communication link to the Security Center is temporarily lost, smart processors can store data locally for transmission later, after the link is restored.

(5) The number of local processors required for a specific site depends on the number of protected areas and their proximity to each other and the number of sensors within a protected area. For example, a small building may require one local processor, whereas a large building may require

one or more for each floor. An external IDS perimeter with two or three different sensors may require one local processor for every two perimeter zones. All local processors may be linked to the central computer using one common DTM link, or the DTM may consist of several links. The designer should note that the temporary loss of a DTM link will render all local processors on that link inactive for the loss duration. Diagrams of typical local processor arrangements are shown in figure 6-4. The top portion of the figure uses one communication link. This arrangement places a 100 percent communication burden on DTM link integrity. The center portion depicts a ring configuration capable of bilateral communications. The bilateral ring will provide uninterrupted communication in the event of a single point failure such as a ring cut. The bottom portion depicts a redundant bilateral ring DTM where each ring connects to every local processor. This arrangement can be used in high security applications where, for maximum effectiveness, the redundant rings are physically separated so that a single point failure on both rings and a loss of communication on one ring will not disable IDS device communications to the Security Center.

b. IDS central computer and local processor data exchange. Upon IDS power up or system reset at the Security Center, the IDS central computer will down-load all necessary IDS operational information over the DTM to all local processors. Upon completion of down-load, the central computer will automatically begin polling the local processors for IDS device status. In addition to alarm status, tamper indications, and local processor status, the DTM may be required to convey Security Center console operator commands to field devices. Examples include—

(1) Security area access/secure mode changes.

(2) Initiate IDS sensor self test.

c. Error detection and retransmission. A significant amount of binary data is transmitted over the DTM to maintain Security Center contact and control over IDS field devices. To safeguard binary data integrity, the designer must consider a method to detect corrupted messages. Methods available range from reliance on Security Center console operator detection to automatic detection, correction, and retransmission of corrupted messages. Reliance on console operator detection is not recommended for Army installations. The designer will specify an automatic error detection method compatible with the value of the assets protected by the IDS.

6-6. DTM

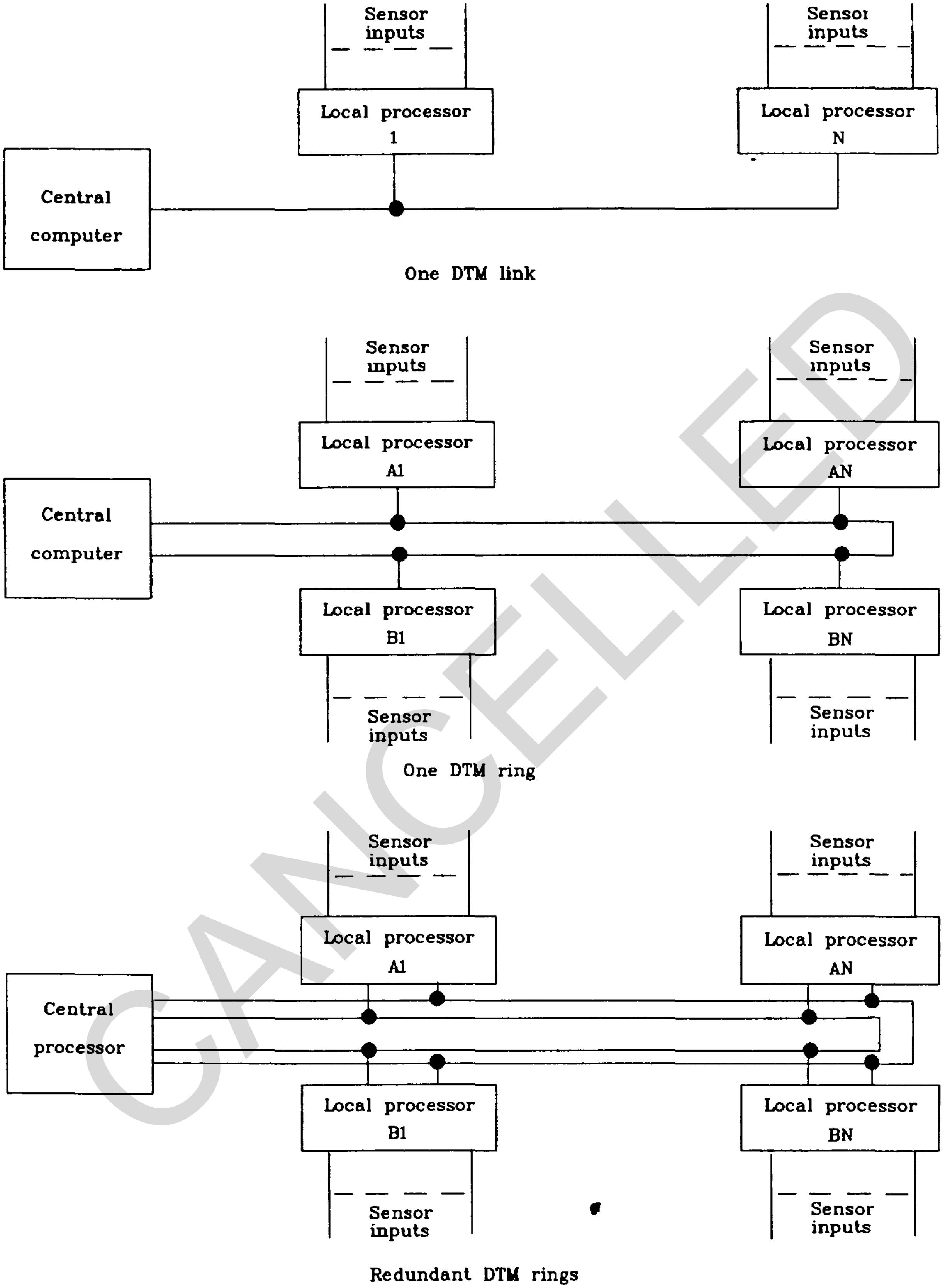
The requirement for the Security Center to communicate with field deployed devices over the DTM must be addressed for any IDS design. For smaller systems, DTM supervision will be provided by the central computer itself. As the IDS system size grows, DTM supervision may be delegated to a hardware module separate from the central computer. For very large systems, a DTM network may be used. This network would deploy data concentrators at key locations throughout the facility and communicate with a security console communication processor over high-speed DTM links. Information flow between the communication processor and the field devices is usually accomplished by serial transmission. Serial transmission requires a single communication line per link (a pair of wires or a single optic fiber). The most commonly used serial transmissions are specified by the EIA RS-232 and EIA RS-422 standards. Additional information concerning DTM design is presented in chapter 9.

6-7. CCTV Interface

If a CCTV assessment system is deployed with the IDS, an interface between the two is required. This interface allows CCTV system alarms, such as loss of video, to be displayed by the IDS alarm annunciation system. The interface also provides IDS alarm signals to the CCTV video switcher so that the correct CCTV camera will be displayed on the CCTV monitors to allow real-time alarm assessment and video recording as required. Additional information concerning CCTV design is presented in chapter 8.

6-8. EECS Interface

If an electronic entry control system is deployed with the IDS design its interface is an essential component of an IDS. It should inform the Security Center console operator of an abnormal ingress or egress transaction occurring at any controlled area. It should also inform the Security Center console operator that a touring guard is overdue at a particular security area. Additional information concerning electronic entry control system design is presented in chapter 7.



One DTM link

One DTM ring

Redundant DTM rings

Fıgure 6–4 Multıplexed DTM Configuratıons

Section II. SOFTWARE

6–9. Types of Software

The software provided with computer-based IDS alarm annunciation systems consists of two sets of programs: a standard operating system (system software), like MS–DOS and vendor developed application programs.

a. System software. The designer will ensure that system software provided by the vendor conforms to accepted industry standards so that standard, follow-on maintenance and service contracts can be negotiated to maintain the central computer system.

b. Application software. The vendor-developed application programs are typically proprietary and include data structures by which the user can specify the IDS device configuration. The data structures are then used to specify site-specific IDS monitoring, display, and control requirements. Vendors' application programs and data structures are typically written in a programming language that is compiled to produce a machine language program. The application program and data structures, in their pre-compiled form, are referred to as source code. The output of source code compilation is called object code; this is the instruction set that controls the central computer. Object code is very difficult to analyze or modify. The designer will ensure that the software vendor will provide future software maintenance and support or, as a minimum, makes available an annotated, computer readable copy of the source code.

c. Enhancement software. Enhancement software can associate supplemental information with incoming alarm messages. This information may include preferred route descriptions for the response force, the phone number of the person responsible for the alarmed area, and any hazardous materials that may be located in the alarmed area. Software can provide automated documentation of a developing alarm incident; an incident starts with the annunciation of an alarm and ends when the console operator supplies the final disposition for that alarm. The software typically displays a blank incident form on a monitor screen. The central computer supplies information into the form as it becomes available during the developing incident (time of acknowledge, time of reset). The operator supplies only those portions of the form information that the computer does not know; typically, the final disposition of the alarm and any ancillary comments. When the incident form is completed, it becomes part of the system data base and is, therefore, available for hard-copy or to be included in summary reports for security management.

6–10. Software Functions

In evaluating - data structures and software requirements, the designer will ensure that the application software provides the following functions.

a. Alarm monitoring and logging. The software should provide for monitoring all sensors, local processors, and data communication links, and notifying the operator of an alarm condition. All alarm messages should be printed on the alarm printer and displayed at the console. As a minimum, printed alarm data should include the date and time (to the nearest second) of alarm and location and type of alarm.

b. Alarm display. The software should be structured to permit several alarms to be annunciated simultaneously. A buffer or alarm queue should be available to store additional alarms until they are annunciated and, subsequently, acted upon and reset by the console operator.

c. Alarm priority. A minimum of five alarm priority levels should be available. Higher priority alarms should always be displayed before lower priority alarms. This feature permits an operator to respond quickly to the more important alarms before those of lesser importance. For example, the priority of alarm devices could be as follows:

(1) Duress.

(2) Intrusion detection.

(3) Electronic entry control.

(4) Tamper.

(5) CCTV alarms and equipment malfunction alarms.

d. Passwords. Software security will be provided using passwords to limit access to personnel with authorized passwords assigned by a system manager. A minimum of three password levels shall be provided. Additional security can be provided by programmed restrictions that limit the keyboard actions of logged-in passwords to the user ranks of system manager, supervisors, and console operators, as appropriate.

e. Operator Interface. The software should enable an operator with the proper password to enter commands and to obtain displays of system information. As a minimum, an operator should be able to perform the following functions through the keyboard or the keypad.

(1) Log on by password to activate the keyboard.

(2) Log off to deactivate the keyboard.

(3) Request display of all ke)board commands that are authorized for the logged-in password.

(4) Request display of detailed instructions for any authorized keyboard command.

(5) Acknowledge and clear alarm messages.

(6) Display the current status of any device in the system.

(7) Command a status change for any controlled device in the system.

(8) Command a mode change for any access/secure device in the system.

(9) Command printouts of alarm summaries, status summaries, or system activity on a designated printer.

(10) Add or delete IDS devices or modify parameters associated with a device.

f. Reports. The application software should provide for the generating, displaying, printing, and storing of reports on disk or tape. As a minimum, the following reports should be provided:

(1) An alarm report, showing all alarms annunciated by the system by type of alarm (intrusion, tamper, etc.), type of sensor, location, time, and action taken.

(2) A system test report documenting the operational status of all system components after a system test.

(3) An access/secure report documenting all zones placed in access, the time placed in access, the time a zone was returned to the secure mode, and the person commanding the change.

(4) The number of alarms reported by a specific zone over a specified period of time.

(5) Event tracking showing all alarms and operator response.

g. Response force guidance. Software data structures will provide the operator guidance in response deployment based on alarm area information. Examples are—

(1) Area point of contact, name and phone number.

(2) Best response force route to alarmed area.

(3) Description of area contents.

6-11. CCTV Interface

If the IDS includes CCTV assessment cameras, the IDS software will provide the commands required by the CCTV video switcher to call up the alarm correlated video camera for display and recording. The interface will also allow CCTV system alarms to be displayed on the IDS console.

6-12. EECS Interface

If the IDS includes an electronic entry control system, software will provide for the exchange of information between the alarm annunciation processor and the electronic entry control system processor. Examples are—

a. Area X reports equipment tamper.

b. Area X reports forced entry.

c. Area X reports out-of-service.

d. Area X reports emergency crash-out exit.

Section III. RELIABILITY

6-13. Reliability Considerations

Computer reliability can be viewed from three aspects. First, reliability can be improved by protecting the computer from unauthorized access, tampering, and attack. Second, from the console operator's point of view, IDS reliability increases as the number of false alarms decreases. Finally, in the traditional sense, reliability increases as the mean-time-between-equipment-failure increases. Each aspect will be considered by the designer.

a. Protecting the computer. The computer and its DTM line termination equipment should be located in a controlled area and provided with tamper protection. Changes to software should be permitted by supervisory personnel only and such changes should be documented. If redundant DTM links connect the central computer to the local processor, diverse paths should be employed to route these links.

b. Reduce false alarms. The central computer should impose integrity checks on incoming alarm messages as a condition of their annunciation. Examples of integrity checks include requiring duplicate, and identical messages, or reception of a message followed immediately by its inverse, and appending framing and parity bits to all message transmissions. The central computer should report sources of unusually high numbers of defective messages to the console operator so that they may be repaired or replaced by maintenance personnel.

c. Reduce equipment failures. Improvements in integrated semiconductor fabrication techniques have been somewhat offset by expanding processor capabilities; the average gate count per processor function has been increasing. To mitigate this increase in complexity, a central computer will include self-diagnostic routines designed to provide advance warning of pending module failure or actual failure. In more sophisticated designs, the central computer will also, at preprogrammed intervals, issue self-test commands to the various IDS sensors and verify that appropriate responses are being received.

d. Fault-tolerant computer systems. If the value of the assets being protected warrants the additional cost, redundant, fault-tolerant central computer systems will be specified. One arrangement is referred to as the "Hot-Standby" configuration. In it, two peer processors are provided; one is designated the main, the other the backup. At any given time the main has control of the console output devices. Also included is a failover controller that monitors both units. The failover controller continually compares the progress and timing signals of each computer. Figure 6–5 is a block diagram of a typical redundant central computer system incorporating a failover controller. Because the computers share identical input information (stimuli), their outputs should always be in agreement. Should a discrepancy arise, the failover controller disconnects the main computer from the output devices, replaces it with the backup, and informs the operator that the main computer is no longer available.

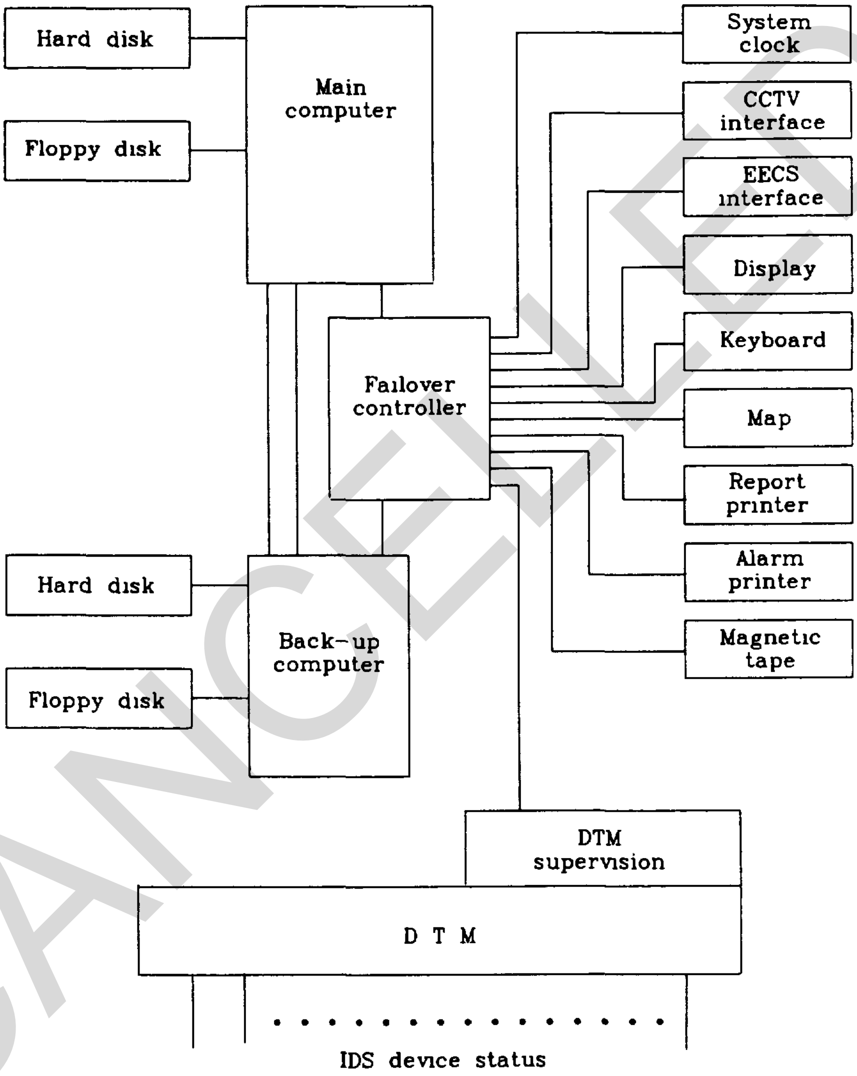


Figure 6–5. Typical Redundant Computer Configuration.

CHAPTER 7

ELECTRONIC ENTRY CONTROL

Section I. TYPES OF ENTRY CONTROL DEVICES

7–1. General

a. The function of an entry control system is to ensure that only authorized personnel are permitted ingress to or egress from a controlled area. Entry can be controlled by means of locked fence gates, locked doors to a building or rooms within a building, or specially designed portals.

b. These means of entry control can be applied manually by guards or automatically through use of entry control devices. In a manual system, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics described on an identification badge with characteristics of the individual requesting entry. In an automated system, the entry control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage. This chapter discusses electronic devices and systems used for automatic entry control. Mechanical hardware, such as locking mechanisms, electric door strikes, and specially designed portal hardware, and equipment used to detect contraband material, such as metal detectors, X-ray baggage search systems, explosives detectors, and special nuclear material monitors, are described in other documentation. Refer to TM 5–853–1 for additional information on determining entry control requirements and integrating manual and electronic entry control into a cohesive system.

c. All entry control systems control passage through use of one or more of three basic techniques, based on something a person knows, something a person has, or something a person is or does. Automated entry control devices based on these techniques are grouped into three categories: coded devices, credential devices, and biometric devices.

7–2. Coded Devices

These devices operate on the principle that a person has been issued a code to enter into the entry control device that will match with the code stored in the device and permit entry. Depending on the application, a single code can be used by all persons authorized to enter the controlled area or each authorized person can be assigned a unique code. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas. Coded devices verify authenticity of the code entered and any person entering a correct code is authorized to enter the controlled area. Electronically coded devices include electronic keypads and computer-controlled keypads. Mechanically coded devices, such as combination locks and mechanical cipher locks, are described in other documentation.

a. Electronic keypad devices. The common telephone keypad (12 keys) is an example of an electronic keypad. This type of keypad consists of simple push button switches that, when depressed, are decoded by digital logic circuits. When the correct sequence of buttons is pushed, an electric signal unlocks the door for a few seconds.

b. Computer-controlled keypad devices. These devices are similar to electronic keypad devices, except that they are equipped with a microprocessor internal to the keypad or in a separate enclosure at a different location. The microprocessor monitors the sequence in which the keys are depressed and may provide additional functions, such as personal identification and digit scrambling. When the correct code is entered and all conditions are satisfied, an electric signal unlocks the door.

7–3. Credential Devices

A credential identifies a person as having legitimate authority to enter a controlled area. A coded credential (plastic card or key) contains a prerecorded, machine-readable code. An electric signal unlocks the door if the prerecorded code matches code stored in the system when the card is read. Like coded devices, credential devices only authenticate the credential; it assumes a user with an acceptable credential is authorized to enter. Various technologies are used to store the code upon or within a card. The most common types of cards are described below.

a. Hollerith cards. Data are coded on the card by a series of punched rectangular holes. The card reader contains either an array of electrical contact brushes or an array of light sources or photodetectors. Because of the relative simplicity in duplicating the Hollerith card, it is seldom used for entry control in military installations.

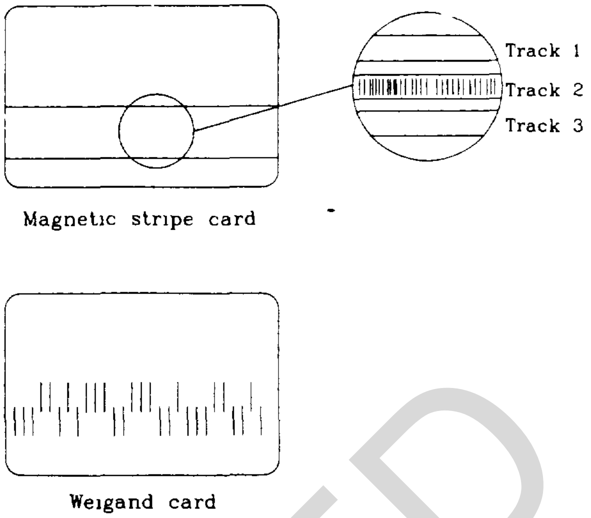
b. Optically-coded cards. Data are encoded on the card through a series of spots that have different levels of transparency when illuminated with a specific type of light. The card reader contains an array of light sources and photodetectors. When a card is inserted into the reader, the photodetectors sense the relative transmissivity of the spots and translate them into the identification number of the card. To provide protection against tampering and counterfeiting, the card can be printed with ink that is opaque to visible light but presents a different level of transparency to infrared light. Alternatively, several levels of transparency may be used so that the optical transmissivity of the spots must fall within a specified range in order to be recognized as a valid code.

c. Electric-circuit cards. The electric-circuit card contains a printed circuit board, laminated between two layers of opaque plastic, with electrical contacts at one end. Data are encoded by selectively opening or shorting the printed circuit pattern. The card is read by inserting it into a card reader, which examines electrical continuity between contacts at the edge of the card.

d. Magnetic-spot cards. The magnetic spot card contains a sheet of flexible magnetic material, such as barium ferrite, on which an array of spots has been permanently magnetized. The code is determined by the polarity of the magnetized spots. The card reader contains magnetic sensors that are interrogated electrically or magnetic reed switches that are mechanically actuated when a magnetic spot with the proper polarity is located adjacent to the reed.

e. Magnetic-stripe cards. A strip of magnetic material located along one edge of the card is encoded with data (sometimes encrypted). The data are read by moving the card past a magnetic read head. Many vendors manufacture and encode the card in accordance with ANSI X4.13 and X4.16 standards. Two materials are commonly used for the magnetic-stripe medium, a 300-oersted tape and a 4,000-oersted tape. The 4,000-oersted tape is much less susceptible to accidental erasure and can tolerate a greater separation between the tape and read head. A typical magnetic-stripe card is illustrated in figure 7-1.

f. Wiegand-effect cards. The Wiegand-effect card, also depicted in figure 7-1, contains a series of small-diameter, parallel wires, approximately one-half inch long, embedded in the bottom half of the card. The wires are manufactured from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. The placement of wires above and below an imaginary center line determine the specific information, which represents a "1" or "0" in binary code. Dummy wires may also be embedded, so that the position of the coded wires is less easily detected. This type of card is impervious to accidental erasure. The card reader contains a small read head and a tiny magnet to supply the applied magnetic field. It usually does not require external power.



Magnetic stripe card

Weigand card

Figure 7-1. Magnetic Stripe and Wiegand-Effect Cards.

g. Capacitance cards. A capacitance card contains a high-dielectric material laminated between two sheets of plastic. Data are encoded by punching holes in the dielectric material, thus reducing capacitance at hole locations. The data are usually encoded in a row-and-column array. The card reader measures capacitance at specific locations of the array.

h. Proximity cards. This type of card is not physically inserted into a reader; the coded pattern on a card is sensed when it is brought within several inches of the reader. Several techniques are used to code cards. One technique uses a number of electrically tuned circuits embedded in the card. Data are encoded by varying resonant frequencies of the tuned circuits. The reader contains a transmitter that continually sweeps through a specified range of frequencies and a receiver that senses the pattern of resonant frequencies contained in the card. Another technique uses an integrated circuit embedded in the card to generate a code that can be magnetically coupled or electrostatically coupled to the reader. The power required to activate embedded circuitry can be provided by a small battery embedded in the card or by magnetically coupling power from the reader.

i. Laser cards. The optical memory card, commonly called the laser card, uses the same technology developed for recording video and audio disks for entertainment purposes. Data are recorded on the card by burning a microscopic hole (using a laser) in a thin film covering the card. Data are read by using a laser to sense the hole locations. The typical laser card can hold up to several megabytes of user data.

j. Smart cards. Embedded in the smart card are a microprocessor, memory, communication circuitry, and a battrery. The card contains edge contacts that enable a reader to communicate with the microprocessor. Entry control information, as well as other data, may be stored in the memory of the microprocessor.

k. Bar codes. A bar code consists of black bars printed on white paper or tape that can be easily read with an optical scanner. This type of coding is not widely used for entry control applications because it can be so easily duplicated. It is possible to conceal the code by applying an opaque mask over it. In this approach, an infrared scanner is used to interpret the printed code. For low level security areas, the use of bar codes can provide a cost effective solution for entry control. Coded strips and opaque masks can be attached to existing identification badges, alleviating the need for complete badge replacement.

7–4. Biometric Devices

The third basic technique used to control entry is based on measurement of one or more physical or personal characteristics of an individual. Because most entry control devices based on this technique rely on measurements of biological characteristics, they have become commonly known as biometric devices. Characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood vessel patterns all have been used for controlling entry. Typically, in enrolling individuals, several reference measurements are made of the selected characteristic and then stored in the device's memory or on a card. From then on, when that person attempts entry, a scan of the characteristic is compared with the reference data template; if a match is found, entry is granted. Rather then verifying an artifact, such as a code or credential, biometric devices verify a person's physical characteristic, thus providing a form of identity verification. Because of this, biometric devices are sometimes referred to as personnel identity verification devices.

a. Fingerprints. Fingerprint verification devices use one of two basic approaches. One is pattern recognition of the whorls, loops, and tilts of the referenced fingerprint, which is stored in a digitized representation of the image and compared with the fingerprint of the prospective entrant. The second approach is minutiae comparison, which means that the endings and branching points of ridges and valleys of the referenced fingerprint are compared with the fingerprint of the prospective entrant.

b. Hand geometry. Several devices are available that use hand geometry for personnel verification. These use a variety of physical measurements of the hand, such as finger lengths, finger curvature, handwidth, webbing between the fingers, and light transmissivity through the skin to verify identity. Both two- and three-dimensional units are available.

c. Handwriting. Although signature comparison is an old and traditional method of identifying a person, there are no completely automated signature comparison machines available. There are many machine-assisted methods, such as provided by CCTV, microfilm, microfiche, and facsimile equipment; however, none of these methods is used at the present time for entry control. For entry control applications, there are several machines that rely upon the manner in which a signature is written; that is, the speed, acceleration, and pressure of the pen with which the signing is done are measured and compared with reference data. The actual signature is not used.

d. Voice verification. Automatic voice verification is a process by which a device authenticates the claimed identity of a person from voice characteristics. Such features of the voice as resonance, pitch, and loudness can be isolated as belonging to a specific person. All voice verification systems use data collected from an individual who repeats certain words or phrases a number of times. To prevent substituting a recording for the voice of an authorized person, the system may generate a random sequence of words, which the person is requested to repeat. The data are then analyzed and compared with reference data.

e. Retinal patterns. This device is based on the premise that the pattern of blood vessels on the human eye's retina is unique to an individual. While the eye is focused on a visual target, a low-intensity infrared light beam scans a circular area of the retina. The amount of light reflected from the eye is recorded as the beam progresses around the circular path. Reflected light is modulated by the difference in reflectivity between blood vessel pattern and adjacent tissue. This information is processed and converted to a digital template that is stored as the eye's signature. Users are allowed to wear contact lenses; however, glasses should be removed.

7-5. Device Combinations

Frequently, an automated entry control system uses combinations of the three types of entry control devices. Combining two different devices can significantly enhance the security level of the system. In some cases, combining devices results in reduced verification times.

a. Keypad and credential. Electronic keypads are commonly combined with credential devices to provide a higher level of security. With this arrangement, the user must present a coded credential to the reader and enter a code, commonly referred to as a personal identification number (PIN), through the keypad. The device processor compares both the credential identification number and the personal identification number with reference data stored in memory. Alternatively, the processor may derive the PIN from information stored on the credential and compare it with code entered via keypad. If the processor verifies both credential and coded entry, a signal unlocks the door.

b. Keypad and biometric. Electronic keypads are commonly combined with biometric devices to reduce verification time of biometric devices. Typically, an individual enters a PIN, which the device processor uses to retrieve that individual's biometric reference template from memory. This template is then compared with data from current measurement of the physical characteristic. If the processor is required to compare measured data with every reference template stored in memory, the time required for verification may increase significantly.

c. Credential and biometric. Coded credentials can also be used with biometric devices. In most cases, information on the credential is used for quick retrieval of the reference biometric template, similar to use of a keypad (see preceding paragraph). However, in some applications, the reference data template is actually encoded on the credential, not in processor memory, so that the measured data are compared with data on the credential. With the latter technique, data are more vulnerable to tampering and counterfeiting than when data are stored in processor memory.

Section II. APPLICATION GUIDELINES

7-6. Site Specific Factors

This section provides guidelines to assist the designer with selection of a site-specific entry control system. It describes a number of available entry control functions, as well as criteria used to evaluate performance of entry control systems. It also describes specific features or attributes of the three types of entry control devices that should be examined during the selection process. Techniques for configuring devices into a system that enable overall command and control are described. This section concludes with a discussion of economics to be considered in design and selection of an entry control system.

7-7. Automated Entry Control System Functions

The primary function of an automated entry control system is to permit ingress to or egress from a controlled area by authorized individuals. Features available to the designer are described below.

a. Enrollment. All entry control systems must provide a means of entering, updating, and deleting information about authorized individuals into the system database files. This is usually accomplished with a dedicated enrollment station that consists of a keypad and monitor used exclusively for enrolling and disenrolling purposes that are directly connected to the central processing unit. When credential devices are used, all authorized users must be provided with an appropriate credential. A means should also be provided to disenroll a person quickly without having to retrieve a credential. When using biometric devices, additional enrollment equipment will be required.

b. Entry control techniques. Some entry control functions require additional hardware, while others are accomplished with software. Those features accomplished with software require that the appropriate data base be available for every portal affected by them.

(1) *Area zones.* For facilities having several different controlled areas, it may be necessary to control entry into each area selectively. Thus, a person authorized to enter one area may not be allowed to enter other areas. This can be accomplished by issuing separate codes or credentials for each area. A more sophisticated approach is to have the system use the person's ideentification number to determine which areas the person is authorized to enter. This approach requires the system to store area zone data and have it available for every entry control point.

(2) *Time zones.* The time zone feature allows the system to control intervals of time during which an individual is authorized to enter an area. For example, the system may be set up to permit a specific individual to enter an area only between 0700 and 1700. Attempted entry at other times is rejected by the system. Some systems provide sixty-four or more time zones. The number of time zones required depends primarily on the number of working shifts at the installation and the number and frequency of overtime work assignments. Time zone control is strictly a software function and requires no additional hardware.

(3) *Team zones.* In areas containing assets that require a very high level of protection, it may be necessary to restrict entry to teams consisting of two or more individuals (two-person rule). Team zoning is a very effective method of protection against the insider threat and is usually accomplished with software.

(4) *Anti-passback.* With keypads and credential devices, it is possible for several persons to use the same PIN or card to enter an area. This can be done, for example, by passing a card from a person entering an area or already inside the area to a person outside. To prevent this, some systems offer an anti-passback feature in which the PIN or card code is remembered when used to enter and cannot be used again to enter until it has first been used to exit. Alternatively, some systems keep track of entry and exit by recording and subsequently erasing a code on the card. Anti-passback usually requires a separate exit device in addition to the entry device. Anti-passback can be implemented on an area by area basis or can be system wide. If system-wide anti-passback is required, a centrally controlled system, discussed later in this chapter, will be required.

(5) *Anti-tailgate.* Tailgating (also known as piggybacking) is a method by which an unauthorized person closely follows an authorized person into a controlled area. Tailgating can be minimized by assuring that all entry control devices are provided with an adjustable time function to control the length of time the door remains unlocked. A door sensor should be included to generate an alarm if the door is not closed within the prescribed interval of time. The most effective means of controlling tailgating is to use turnstiles or mantraps.

(6) *Guard tour.* This is used to monitor a security's guard's progress while making rounds through a facility and is done by having the guard check in at designated entry control devices throughout the facility. The system monitors the time at which a guard arrives at each predefined check point; if the guard is late, an alarm is initiated. If the guard tour feature is necessary, the number of different, simultaneous routes that a system can accommodate, as well as the number of variations that can be set up for each route, should be determined. Guard tours are implemented with software.

(7) *Elevator control.* Some entry control systems provide capability to control elevator operation with entry control devices. These systems usually provide a means to define which floors of a building are to have controlled entry. Unauthorized persons are denied entry to these floors.

c. Occupant list. If the system is designed to keep track of persons entering, as well as exiting, an up-to-date list of persons in the controlled area can be maintained. In the event that an area must be evacuated because of an emergency, a list of those in the area can be obtained, enabling security personnel to verify whether all occupants had cleared the area. In addition, security personnel use this feature to verify that an area is empty before securing it during a nonoperational period.

d. Alarms. Several different types of alarms can be used with an entry control system. These alarms must annunciate both audibly and visually in the Security Center. If the EECS is being installed in conjunction with an IDS, these alarms will be displayed on the IDS alarm monitor by means of an interface with the IDS alarm annunciation system. Following are descriptions of several of the more common types of alarms.

(1) *Entry denial.* Most entry control devices are configured to permit the user up to three entry attempts. If more than three unsuccessful entry attempts are made within a specified period of time, the device generates an alarm. An alarm is also generated if an invalid credential is used, or attempted entries are detected that violate specified area, time, or team zoning requirements.

(2) *Communication failure.* This alarm is generated when a loss of communication between the central processor and local equipment is detected.

(3) *Portal open.* If a portal door remains open longer than a predefined time, an alarm is generated.

(4) *Duress.* This alarm is generated when a special duress code is entered at a keypad.

(5) *Guard overdue.* This is a duress type alarm that is generated when a security guard is determined to be overdue at a check point during a predefined guard tour.

(6) *Software tamper.* This type of alarm is generated when unauthorized persons are detected attempting to invoke certain system commands or modify database files.

7-8. Performance Criteria

The overall performance of an entry control system can be evaluated by examining the verification error rate and throughput rate.

a. Verification errors. An entry control system can produce two types of errors: denial of admission to a person who should be admitted or admission of a person who should not be admitted. These are commonly referred to as false-reject errors (type I errors) and false-accept errors (type II errors), respectively. Although a false-reject error does not constitute a breach of security, it does create an operational problem that must be handled by an alternative method. False-accept errors definitely constitute a breach of security. Ideally, both false-reject and false-accept error rates should be zero; in practice, however, they are not. In fact, they tend to act in opposition to each other. When the system is adjusted to minimize the false-accept error rate, the false-reject error rate usually increases. Verification error rates are typically measured in percent (number of errors/number of attempts x 100 percent). These error rates are typically very low for coded and credential devices but may become significant if biometric devices are employed.

b. Throughput rate. The throughput rate is the number of persons that can pass through an entry point in a given unit of time, and is usually expressed in persons-per-minute. It is a function of time required to approach the entry control device, time required to enter information into the device and for the device to verify information (verification time), and time required to pass through the entry point. Typically, an individual can approach the device and pass through in 3 to 5 seconds. Verification time depends on the type of device and may vary from 3 to 15 seconds. Table 7-1 provides a list of typical verification times for different types of entry control devices.

Table 7-1 Typical Verification Times of Entry Control Devices

Device	*Verification Time*
Keypad	3 seconds
Card reader	3 seconds
Keypad/card reader	6 seconds
Biometric/keypad	6-15 seconds
Biometric/card reader	6-15 seconds
Biometric	2 minutes

7-9. Coded Device Considerations

When selecting keypads for entry control, several factors should be considered. These include the number of possible combinations allowed, methods to improve the security of the keypad, code-change procedure, and duress alarm capability.

a. Number of combinations. Level of security provided by a keypad is highly dependent upon the number of available combinations. For example, if only 1 digit must be entered on a 10-digit keypad, a person has a 1-in-10 chance in obtaining entry, even if the correct number is unknown. If two digits are required, the odds on obtaining entry are one in a hundred, and for three digits, the odds increase to one in a thousand. The number of possible combinations provided by a keypad depends not only on the number of key depressions required to enter the code but also on the number of keys provided, whether a key may be used more than once in the code sequence, and whether or not a number of keys may be depressed at the same time.

b. Defense methods. The simplest method of attacking a keypad entry control device is to try all of the possible combinations until the correct one is found. This can be done all at one time if the keypad is located in an unattended area or it may be done over a period of days or weeks by trying a few combinations at a time. There are several different ways of defending against this weakness.

(1) Increasing the number of possible combinations will increase the amount of time required to enter all possible codes. The odds of selecting an authorized code are dependent on the relative number of assigned codes compared to the total number of possible codes, not just the total number of codes the system can accommodate. For example, if the system allows 100,000 possible codes and only 100 are assigned, the odds are 1 in a 1,000 that a correct code will be entered on any given attempt. If each attempted entry takes 3 seconds, it should take an intruder approximately 50 minutes to stumble across a correct code. On the other hand, if 20,000 codes are assigned, the odds of randomly selecting an authorized code drop to 1 in 5, which means an intruder can theoretically stumble upon a correct code in 15 seconds or less.

(2) Changing the required code frequently enhances security of the keypad. However, all authorized entrants must be notified each time the code is changed.

(3) Another approach is to provide an adjustable time penalty that will deactivate the keypad for a period of time after an unsuccessful code entry. This feature increases the amount of time required to enter all possible combinations but also reduces throughput.

(4) The security of a keypad can be considerably enhanced if an alarm is generated after an

incorrect code entry. Because authorized personnel sometimes may enter a code incorrectly, an alarm is usually not generated until at least three successive incorrect entries are made.

c. Code changing. As mentioned previously, frequently changing the code enhances security of the keypad. Hence, ease and time required to change the code physically should be examined. If jumpers or switches are used to set the code, tamper protection must be provided. If the code is stored in electronic memory, safeguards must be provided to protect against power transients or loss of power.

d. Duress alarms. Some systems with keypads provide an individual with capability to generate an alarm secretly while entering the code. This feature is useful if the individual is physically coerced to open the door. The alarm is entered by pressing an additional digit or a designated alternate digit on a keypad during the code entry process.

7-10. Credential Device Considerations.

Characteristics of different credential devices offer a mixture of pro and con attributes, which the designer must consider carefully during the selection process. The ability to decode, alter, or duplicate the credential; the sensitivity of the coding to accidental alteration or erasure; the physical attributes of size, thickness, stiffness, and durability; the amount of coded information; and requirements of manufacturer or user encoding must be considered. Many of these factors, as well as a description of basic types of card readers, are discussed in following paragraphs. A comparison of characteristics of various types of coded credentials is presented in table 7-2.

a. Ease of duplication. Any type of coded credential can eventually be decoded and duplicated. Some are more difficult to duplicate than others, depending on the technology. For example, the material embedded in the Wiegand card is available from only one manufacturer and is difficult to obtain. On the other hand, punching holes in a card to duplicate a Hollerith card is relatively simple.

b. Accidential alteration or erasure. Some types of credential cards can be affected by or can affect the surrounding environment. For example, data on magnetic stripe cards can be erased if brought within a magnetic field. Active proximity cards can affect or be affected by other types of wireless devices.

c. Physical attributes. Most credential cards are the same size as a common credit card, 2-⅛ inches by 3⅜ inches. These cards are subject to considerable wear and tear. For example, a card stored in a wallet is subject to bending, rubbing, and compression. Cards may also be exposed to a wide variety of weather conditions. The useful life of a card depends on the type of material it is made of, as well as the technology used in coding it. Some materials may deteriorate rapidly when exposed to sunlight or heat and become brittle when exposed to cold. However, there are plastic materials that withstand years of daily use without damage. Cards containing active circuitry are more susceptible to damage than cards embedded with a passive material. Surface-coded cards, such as magnetic stripe cards, are more subject to wear than cards with an embedded technology.

d. Code capacity. The number of code combinations available depends on coding technology used and encoding area available on the credential. Code is stored as individual bits of data. One bit provides two combinations; for example, a spot is magnetized or not. Sixteen bits provide 65,536 combinations and 32 bits provide approximately 4.3 billion combinations. The encoding area required per bit may range from 0.01 to 0.25 square inches, depending on the encoding technique. Typically, 16 to 21 bits are required on an entry

Table 7-2. Comparison of Coded Credential Cards

Type of Cards	*Code User Changeable*	*Ease of Duplication*	*Durability*	*Error Rate*	*Cost*
Hollerith	No	Easy	Poor	Low	Low
Optical	No	Mod	Good	Low	Mod
Electric-circuit	No	Easy	Fair	Mod	Low
Magnetic spot	Yes	Mod	Fair	Low	Mod
Magnetic stripe	Yes	Easy	Fair	Mod	Low
Wiegand	No	Mod	Good	Low	Mod
Capacitance	No	Mod	Good	Low	Mod
Proximity	No	Diff	Good	Mod	Mod
Laser	No	Diff	Good	Low	High
Smart	No	Diff	Good	Low	High

Mod - moderate; Diff - difficult.

co,tro' credent:al; additional bits may be provided for personal information.

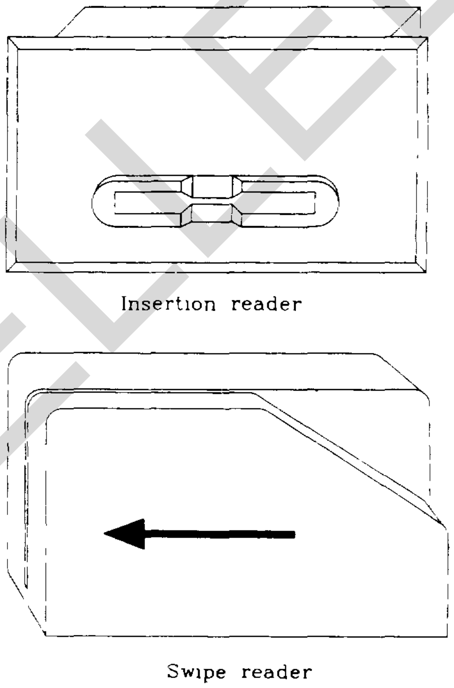
e. Credential coding. An important consideration is whether the user can change code on the credential. In many technologies, the code is built-in during the manufacturing process and cannot be changed. A few technologies, such as the magnetic-stripe credential, permit the user to change the code. Changing codes periodically increases the level of security offered by the system. It is more generally cost effective and convenient to change codes than to purchase all new credentials periodically. However, user-changeable credentials can be duplicated more easily than factory-coded ones.

f. Error rates. In general, coded credentials have very low false-reject and false-accept rates. Errors in reading cards are usually the result of misalignment of the card in the reader, dirt on the reader heads, and bent or dirty cards.

g. Types of card readers. Other than proximity readers, there are two basic types of card readers, the insertion (or slot) reader and the swipe reader. With the insertion reader, the card is inserted into a slot where it passes the read heads and is then ejected by means of a spring or motor drive. With this type of reader, the entire area of the card can be used to store code. With a swipe reader, the user holds the top edge of the card and manually moves it through the reader. Swipe readers are usually bi-directional, that is, they can read the card when it is drawn through in either direction. Although the swipe reader was originally developed for the magnetic stripe card, other credential coding technologies have been adapted for use with the swipe reader. Because of fewer moving parts, swipe readers are more econonomical and more reliable than insertion readers. Examples of a typical insertion reader and swipe reader are shown in figure 7-2. Proximity readers can offer some operational and security advantages over swipe and insertion readers. Since the card does not have to come in contact with the proximity reader, there are no exposed external parts, and they are thus less vulnerable to harsh environmental conditions and vandalism. Also, a person carrying papers or equipment can more easily gain access because they do not have to physically enter the card in the reader.

7-11. Biometric Device Considerations

a. Verification errors. Unlike keypad devices and credential devices, biometric devices can produce significant verification errors (both false-reject and false-accept). This is primarily because of complexity of the measurement technique and variations in ways personal attributes are presented for measurement. Most biometric devices have a sensitivity or threshold adjustment. The false-acceptance error rate can be reduced by increasing sensitivity (lowering the threshold). However, this also results in an increase of false-rejection error rates, which may be acceptable if the authorized user understands that two or three attempts may be required to achieve entry. Figure 7-3 illustrates typical error rate curves for a biometric device.



Insertion reader

Swipe reader

Figure 7-2 Insertion and Swipe Card Readers

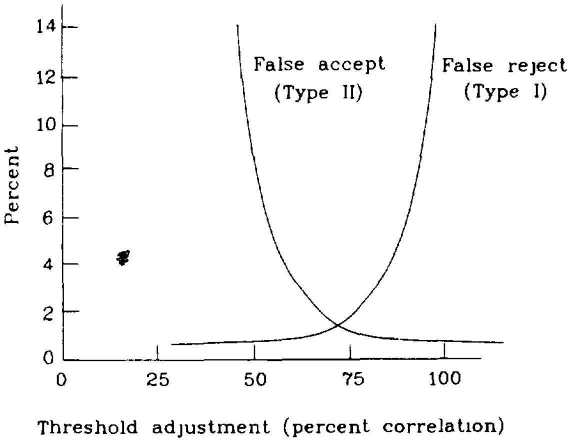


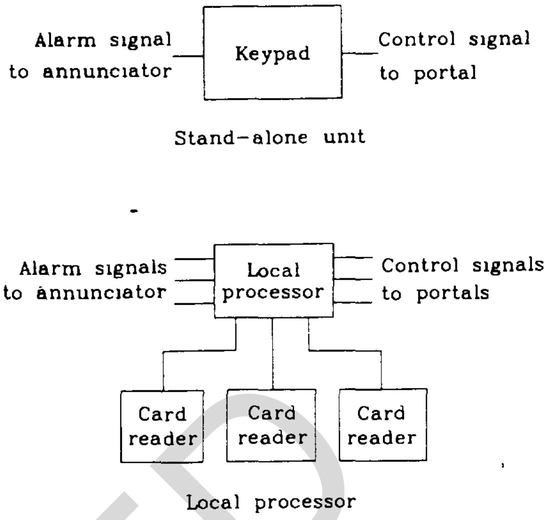
Figure 7-3 Biometric Device Error Rate Curves

b. Enrollment. The enrollment procedure for biometric devices is significantly different than that required for keypad or credential devices. With keypad devices, the security manager issues a code to an enrollee or, depending on sophistication of the keypad system, each enrollee may select his own code, which is keyed into the system. With credential devices, the security manager issues each enrollee a credential, which may be issued as received from the manufacturer or as modified with additional site-specific information. In any case, only a few minutes are required for the enrollment process. User interaction and enrollment time for biometric devices are much greater than for keypad or credential devices. The enrollment process usually begins by briefing the potential enrollee on use and operation of the biometric device. Several reference measurements are then taken of each relevant physical attribute. For example, 5 to 10 samples may be needed for signature verification devices. For hand geometry devices, several measurements with one or both hands may be required. If the biometric devices are networked to a central computer, a dedicated biometric device can be used for enrollment processing. However, if several stand-alone devices are used, the person may have to be enrolled in each individual device. Time required for enrollment in a biometric device is typically about 15 minutes. Experience has shown that some persons can not be enrolled in some types of devices. Other means, such as manual verification by a guard, may be required to allow entry for these persons.

7–12. Command and Control

Command and control functions for an entry control system can be located at each portal or at one or more shared central locations. In some cases, the type of device determines its location. Some types of keypads cannot be controlled from a central location. The number of portals to be controlled and the type of entry control features offered also influence the location of command and control hardware. Several command and control configurations are described in following paragraphs.

a. Self-contained portal units. Device hardware mounted at the portal can contain all intelligence required for command and control. For example, individual doors can each have a stand-alone keypad or card reader. Alarms generated by a stand-alone unit can be annunciated locally or uplinked to a centrally located annunciator. A block diagram of a typical stand-alone unit is shown in figure 7–4.


Alarm signal to annunciator
Keypad
Control signal to portal
Alarm signals to annunciator
Local processor
Control signals to portals
Card reader
Card reader
Card reader

Stand–alone unit

Local processor

Figure 7–4. Local Equipment Configurations

b. Local control. A local processor can obtain command and control functions for several nearby portal keypads or card readers. These processors can function as stand-alone units or they can serve as a means of concentrating communications between portals and a central processor. Alarms from a local processor can annunciate locally or at a central location. Ancillary equipment, such as a keypad and monitor, may be required to enter data into the database. A block diagram of a typical local processor configuration is shown in figure 7–4.

c. Central control. With central control, all command and control intelligence resides in a central processor connected with and controlling all portal equipment. Peripherals, such as a monitor, printer, and magnetic disk or tape system for storing data, are provided with the processor. These devices are similar to those described in detail in chapter 6. Since the central processor is shared by all portals, it is the most economical means of providing sophisticated entry control functions, such as time zoning, area zoning, team zoning, global anti-passback, and occupant lists. Figure 7–5 is a block diagram of an entry control system configured with central control.

(1) *Redundant processors.* With centrally controlled systems, failure of the central processor can cause serious overall system failure. The effect of such failure can be reduced by using redundant processors. With this arrangement, each processor maintains its own copies of system software, application software, and data files. The data files of each processor are updated on a real-time basis. In the event of a failure of the main processor, the redundant (backup or standby) processor automati-

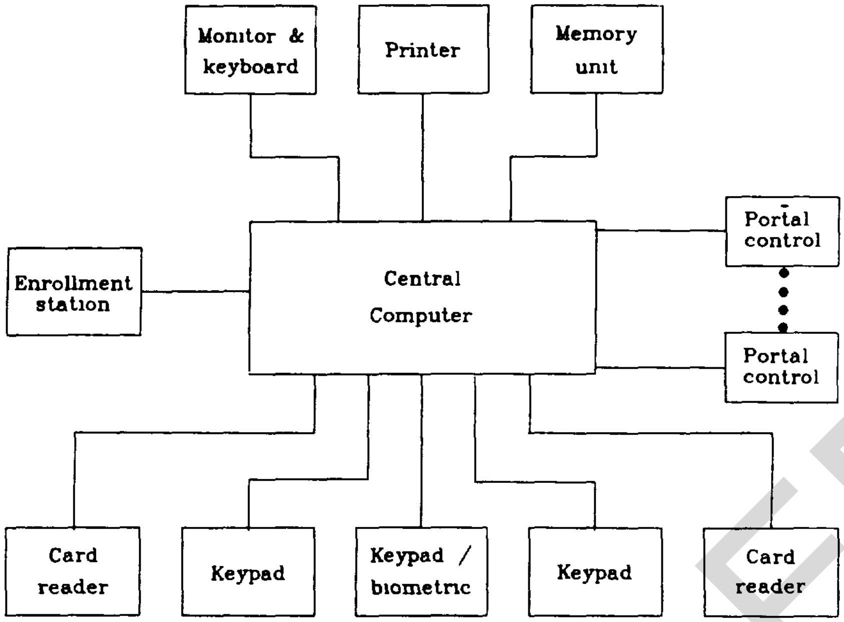


Figure 7–5 Centrally Controlled Entry Control System.

cally assumes responsibility for control of the system.

(2) *Real-time clock.* A real-time clock provides a time stamp for all entry control events. The clock should be settable by the console operator, include battery backup, and be readable by all system devices so that system events are properly time correlated. If an IDS alarm annunciation system is provided, the EECS real-time clock must be synced with the IDS system real-time clock.

(3) *Diagnostics.* The designer should ensure that the central processor contains built-in diagnostics that are implemented in software or hardware. The diagnostics should automatically execute a series of built-in tests and report equipment malfunctions or configuration errors whenever the central processor is started or rebooted.

(4) *Enrollment station.* An enrollment station must be provided to enroll or disenroll a person in the EECS. The station usually consists of a keyboard, monitor, and printer. This station usually provides database management functions that permit an operator to change and modify data as required. A password protection scheme is usually implemented to prevent access by unauthorized persons.

d. Distributed control. In a distributed control type of system, command and control functions are distributed among the central processor and local processors. Although more costly than a centrally controlled system, a well-designed distributed system can continue to operate in a degraded mode. For example, if the central processor fails or if one or more data communication links are lost, the local processors will continue to provide portal control. However, certain functions, such as global anti-passback or personnel tracking (occupant lists), will be lost. Figure 7–6 is a block diagram of an entry control system configured with distributed control. Peripheral devices, such as keyboard, monitor, printer, and magnetic storage devices, are similar to those described in chapter 6.

(1) *Central processor.* The central processor used with a distributed system is similar to that used in a centrally controlled system.

(2) *Local processor.* The local processor is mounted in the field near the portals under its control. It contains a microprocessor, memory, realtime clock, communication ports, and input/output circuitry. The local processor monitors portal status, controls portal operation, and transmits all portal activity information to the central processor.

(*a*) *Capacity.* A local processor controls a combination of electric door strikes, card readers, keypads, and other entry control devices. It must contain enough memory to store a subset of the central processor database sufficient to support employees needing entry through each controlled portal. Expansion modules to support additional entry control devices or memory should be available.

(*b*) *Real-time clock.* Each local processor must include a real-time clock that is synced with

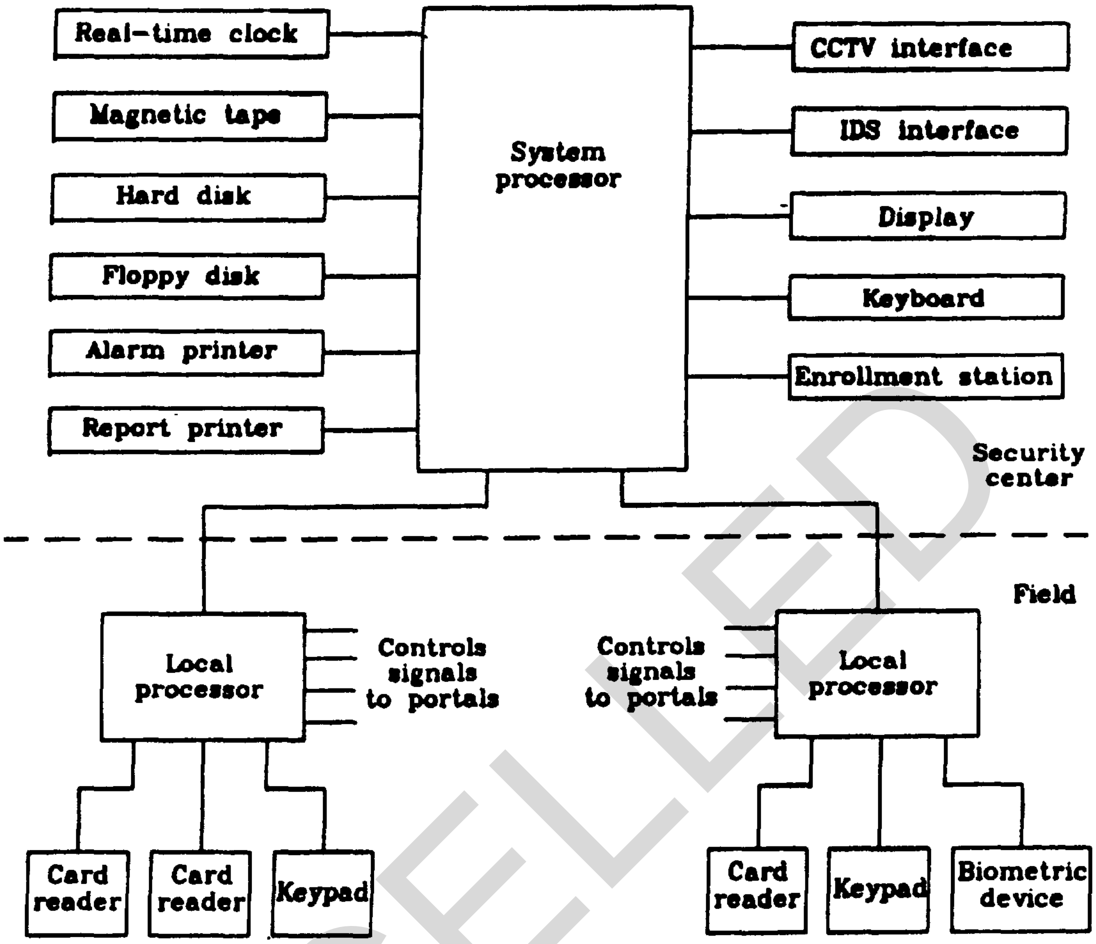


Figure 7-6 Entry Control System Configured With Distributed Control.

the master real-time clock. The master clock may be provided by the EECS central processor or the IDS alarm annunciation system.

(*c*) *Response time.* The local processor must respond to valid ingress and egress requests from its associated entry control devices by generating a signal to unlock the portal within a reasonable period of time, typically within 100 milliseconds after verification. The local processor must also respond to interrogation by the central processor, also typically within 100 milliseconds.

(*d*) *Autonomous local control.* Local processors are usually provided with the capability to automatically convert to autonomous monitoring and control of their associated entry control devices if communication with the central processor is lost. They usually revert automatically to central control upon restoration of communications. The designer should ensure that the local processor has sufficient memory to store system transactions occurring during the communication outage. A good rule of thumb is to provide enough memory to store data from 1,000 transactions.

(*e*) *Diagnostics.* The designer should ensure that the local processor is provided with diagnostics that automatically execute a series of built-in tests during startup. Diagnostic aids should also be provided to assist in maintenance and trouble shooting.

7-13. Economic Considerations

The cost of an entry control system depends on the number of portals to be controlled, type of entry control devices (keypad, credential, biometric), type of control (local, central, or distributed), and the number of system features and options. A stand-alone keypad is the most economical of the electronic entry control devices. The cost of a stand-alone credential device is typically two or three times that of a keypad device. The cost of updating and replacing credentials must also be considered. Biometric devices are the most expensive, typically costing 10 to 20 times as much as a credential device. The many features and options available, such as area zoning, time zoning, anti-passback, occupant list, and logging, will increase the cost of a system. When multiple portals are to be controlled and a large number of additional features and options are desired, a centrally controlled system is the most economical approach, but a distributed system allows for maximum flexibility and the ability to operate in a degraded mode.

Section III. DESIGN GUIDELINES

7-14. Basic Design Criteria

The three most important criteria to be applied in designing an entry control system for a specific site are identification of areas requiring controlled entry, level of security required at each area, and number of persons requiring entry to the area. These three considerations contribute significantly to the type of devices selected, their locations, and the number needed. Visitor control and admission of emergency vehicles are additional criteria to be taken into account.

a. Identification of controlled areas. The first objective of the design process is to identify areas for which entry is to be controlled. Minimum requirements for controlled entry at many different Army facilities are defined in ARs (see B). Types and locations of assets within an installation determine areas that require controlled entry. Site plans and floor plans must be used to identify clearly all existing portals within these areas. The site security manager should be contacted to determine if there are additional areas where controlled entry is required.

b. Security level. Types and values of assets contained within an installation and types and severity of any anticipated threat determine the security level required. The security level of each area within the installation will be classified as level A, B, C, or D in accordance with AR 190-13. The security level determines the IDS sensor requirements and configurations as well as the entry control requirements. For example, a simple keypad does not provide adequate entry control for level A or B facilities; however, it may be adequate for level D facilities. Table 7-3 lists suggested entry control devices for the four security levels and is provided as a guide. The site security officer should be consulted to determine the actual EECS requirements for a specific installation.

Table 7-3. Security Level/Entry Control Matrix

Security Level	*Entry Control Device*
A	Credential and biometric/keypad
B	Credential and biometric/keypad
C	Credential and keypad
D	Credential or keypad

c. Throughput. The number of individuals who require entry to each controlled area and their work schedule should be determined. From this information, the average throughput rate necessary for peak periods, such as shift changes, must be ascertained. If that rate is high, multiple portals may be required to reduce waiting time for those who must obtain entry. In general, the maximum waiting time should not exceed 5 minutes.

d. Visitor control. Practically all facilities must accommodate visitors from time to time. Because visitors can represent a distinct threat, visitor control is necessary and is usually accomplished with administrative procedures. If the site requirements dictate temporary enrollment of visitors into the EECS, then proper software and extra credentials, if required, must be specified. In general, visitor credentials will only allow entry into a specific area during a specific time period; therefore, area and zone software functions will be required as a minimum.

e. Emergency vehicles. In the event of an emergency, fire and rescue equipment and personnel must be allowed to enter and exit a controlled area. The entry control system must be able to accommodate this type of activity, and site-dependent administrative procedures must be accommodated by the designer.

7-15. Equipment Layout and Protection

The integrity of an entry control system depends to a great extent on how the equipment is installed.

a. In considering the layout, the designer must determine whether a highly visible or a low-profile system is required. A highly visible system will serve as a psychological deterrent to an unskilled intruder. However, it will also help to identify areas containing protected assets within an installation. In any case, psychological deterrents very seldom stop determined or skilled intruders; therefore, highly visible systems should be used only in level D security areas.

b. To minimize the potential of someone tampering with circuitry, as much as possible of the entry control equipment should be installed inside the controlled area. Obviously, input devices, such as keypads and credential readers, must be located outside. However, these devices must be installed so that it is impossible to dismantle them from outside the portal. Because they have no exposed external parts, proximity readers provide the best protection against vandalism and tampering. All equipment enclosures must be provided with tamper switches that are positioned so that an alarm is generated before the cover has been moved enough to permit access to circuitry or adjustment controls.

7-16. Other Considerations

Additional factors to be considered when planning and laying-out entry control equipment include effects of the environment on operation of equipment, consequences of power loss, data communication requirements, and expansion capability.

a. Environmental factors. Environmental conditions, such as temperature extremes, high humidity, and dusty conditions, can adversely affect the operation of entry control equipment, usually resulting in an increase of false-reject errors. For example, moisture on certain types of credentials can cause reading errors. Moisture or dirt entering the slot of an insertion reader can damage electronics within the reader. In the case of fingerprint biometric devices, dirt or moisture on the finger can cause reading errors. Entry control equipment for a specific site should be carefully selected and located, to minimize these environmental effects.

(1) *Keypads and card readers.* These devices are available for both indoor and outdoor applications. For indoor applications, they are usually rated to operate over a temperature range of 35 to 120 degrees Fahrenheit and 10 to 95 percent relative humidity, noncondensing. Outdoor devices can be obtained that operate over a temperature range of −30 to 122 degrees Fahrenheit and 10 to 95 percent relative humidity, condensing. Some devices to be used outdoors may require installation in a protective enclosure equipped with a heater.

(2) *Biometric devices.* Biometric devices available at present are designed for operation in interior or protected environments. Most units are designed to operate over a temperature range of 32 to 100 degrees Fahrenheit and a relative humidity range of 10 to 90 percent noncondensing, although a few devices have more restrictive ranges.

b. Loss of power. Consequences of power loss on entry control equipment must be considered. There are two major considerations: personnel safety and portal operation.

(1) Portals can be designed to be either fail-safe (doors unlocked) or fail-secure (doors locked). All portals providing entry to controlled areas will be designed as fail-secure; that is, the doors will remain locked during a loss-of-power condition. However, a power failure must not be allowed to jeopardize personnel safety, such as locking persons irretrievably in or out of the controlled area. A means, such as a key bypass, must be provided to allow entry under failure conditions. All designated exit doors must have a panic bar that allows area occupants to exit in an emergency.

(2) There are several possible methods of handling entry control when primary ac power is lost. The least-cost solution is to provide for operating all portals manually. The doors can be provided with a key bypass or other means to allow entry under failure conditions. Guards or supervisory personnel must then be dispatched to operate portals until power is restored. The most expensive solution is to provide a completely redundant ac power source, such as a gasoline or diesel generator with automatic switchover equipment. An uninterruptible power system is usually necessary to provide power during the time it takes the generator to start and get up to speed, typically 7 to 15 seconds. A more practical solution for many facilities may lie somewhere between the two extremes. An uninterruptible power system may be provided with sufficient battery power to operate the system for several hours. To conserve power, portions of the entry control equipment may be turned off so that the system operates in a degraded mode. The designer must choose a solution that achieves the correct balance of cost and risk for each specific project. Chapter 10 has more information on electrical power sources.

c. Data transmission requirements. When implementing data communication links for an entry control system, both type of medium to be used and data transmission security must be considered. Chapter 9 has more detailed information on data transmission.

(1) The type of media used for data transmission depends on system configuration.

(*a*) For stand-alone configurations, wire lines are usually adequate for connecting the entry control device to its local processor. Because the control device, such as a keypad or card reader, is installed outside of the protected area, wiring must be protected from tampering. This is done by pulling wire in rigid galvanized steel conduit. Additional protection is afforded by embedding the conduit in the wall where the device is mounted.

(*b*) For central processor configurations, data links are required between the entry control devices and the central processor. If the entry control devices and the central processor are installed in the same building, either wire lines or fiber optic cable, installed in rigid galvanized steel conduit, can be used. If the equipment is located in different buildings, direct-burial fiber optic cable may be used for the data links.

(c) For distributed processor configurations, data links are required between the entry control device and local processor and between the local processor and central processor. As with stand-alone configurations, wire lines installed in rigid galvanized steel conduit can be used for the link between the device and its local processor. If the local processor and central processor are located in the same building, either wire lines or fiber optic cable, installed in rigid galvanized steel conduit, can be used. If the processors are located in different buildings, direct-burial fiber optic cable may be used for the data links to the central processor.

(2) Entry control system data links carry data ranging from simple yes/no logic decisions to personal identification information, which can include PIN numbers and personal attribute data, such as fingerprint or retinal scan data. To prevent unauthorized monitoring or tampering, line supervision must be provided for all data links. The facility's security level must be considered when determining requirements for line supervision. For example, simple dc current supervision may be adequate for level D facilities, but for level A facilities, digitally encrypted supervision may be required. Data links crossing an unprotected area typically require more sophisticated line supervision then data links contained completely within a protected area. The designer must balance cost and risk of the selected technique for each specific site.

d. Expansion capability. When specifying an entry control system, the designer must ensure that sufficient expansion capability is provided. The system must have sufficient capacity to control additional portals, as well as accommodate a larger number of people. As a general rule, a minimum of 100 percent expansion should be provided for, since it affects both local processor memory requirements and the size of the hard disk. This additional capacity should be procured as part of the original system.

e. Data classification. Facilities using biometric devices may consider the associated database files to be classified. Other facilities, such as sensitive compartmented information facilities (SCIFs), may consider all entry control database files to be classified. In any case, if the system contains any classified information, the complete system must be handled as a classified system. It may be prudent in large installations to provide two independent entry control systems, one for handling those areas where information is considered classified and one for handling the remainder of the facility.

CHAPTER 8

CCTV FOR ALARM ASSESSMENT AND SURVEILLANCE

Section I. ELEMENTS OF A CCTV SYSTEM

8–1. General

a. Introduction. A properly integrated assessment CCTV system provides a rapid and cost effective method for determining the cause of intrusion alarms. For surveillance, a properly designed CCTV system provides a cost effective supplement to guard patrols. For large facilities, the cost of a CCTV system is more easily justified. It is important to recognize that CCTV alarm assessment systems and CCTV surveillance systems perform separate and distinct functions. The alarm assessment system is designed to respond rapidly, automatically, and predictably to receipt of IDS alarms at the Security Center. The surveillance system is designed to be used at the discretion of and under control of the Security Center console operator. When the primary function of the CCTV system is to provide real-time alarm assessment, the design should incorporate fixed lens cameras and a video processing system that can communicate with the alarm processing system. Because this manual is intended as an aid in the design of electronic security systems, this chapter only addresses the application for CCTV systems to the alarm assessment function. Refer to TM 5–853–1 for guidance on the need for CCTV alarm assessment systems.

b. Site configuration. A candidate site for a CCTV system will typically have the following characteristics:

(1) Assets requiring IDS protection.

(2) Need for real-time alarm assessment.

(3) Protected assets some distance apart.

c. Camera locations. Figure 8–1 depicts a typical CCTV system configuration. A typical site will locate CCTV cameras—

(1) Outdoors, along site perimeter isolation zones.

(2) Outdoors, at controlled access points (sally ports).

(3) Outdoors, within the protected area, viewing approaches to selected assets.

(4) Indoors, at selected assets within the protected area.

d. Security console. The centrally located security console is depicted in figure 8–1. CCTV monitors and ancillary video equipment will be located at this console, as will the IDS alarm processing and annunciation equipment.

8–2. CCTV Camera Components

An optical lens system that caputures and focuses reflected light from the scene being viewed onto an image target is common to all CCTV cameras. The image target converts reflected light energy into electrical impulses in a two-dimensional array of height and width. An electronic scanning system, reading these impulses in a predetermined order, creates a time-sensitive voltage signal that is a replica of optical information captured by the lens and focused on the target. This voltage signal is then transmitted to a location where it is viewed and possibly recorded. Components of the camera are depicted in figure 8–2. The image target and electronics are outfitted with a standard mechanical interface, so that a standard lens assembly appropriate for the scene to be viewed can be used. A CCTV housing protects the lens assembly, image target, and electronics. To provide mechanical stability, the housing is attached to a bracket that is, in turn, anchored to a permanent structure, such as a pole, building face, wall, or ceiling. The light capture and focus function of the lens assembly is a passive optical function, determined by focal length and diameter of the lens. Imaging, scanning, and signal transmission are active electronic functions that require external power. A description of these components follows, including application specific options and enhancements available to the CCTV system designer.

a. Lenses. The optical lens assembly captures and focuses light energy reflected from the viewed scene onto the camera's imaging target. Focal length and diameter are lens parameters that control the capture and focusing of light energy. Both parameters are typically specified in millimeters. The lens system can be optically described as a thin, double-convex lens, which forms images by double refraction of light rays.

(1) *Focal length.* Focal length determines the distance at which light rays, emanating from a point source in front of the lens, will converge and construct an image of that source behind the lens. As with the human eye, the constructed image is inverted. Camera lenses are available as either fixed or adjustable focal length assemblies. An adjustable focal length assembly is commonly referred to as a "zoom lens" and is available as adjustable either at the camera or by an operator

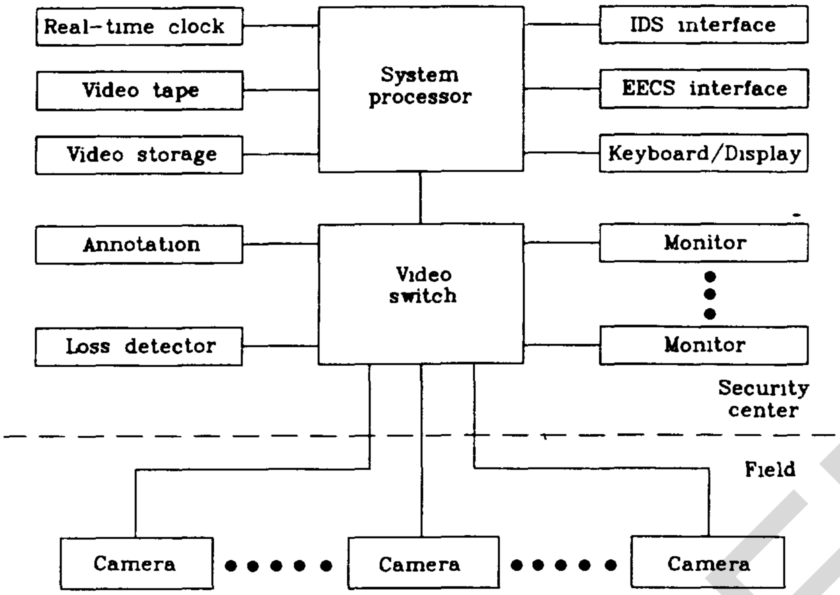


Figure 8-1. Typical CCTV Configuration.

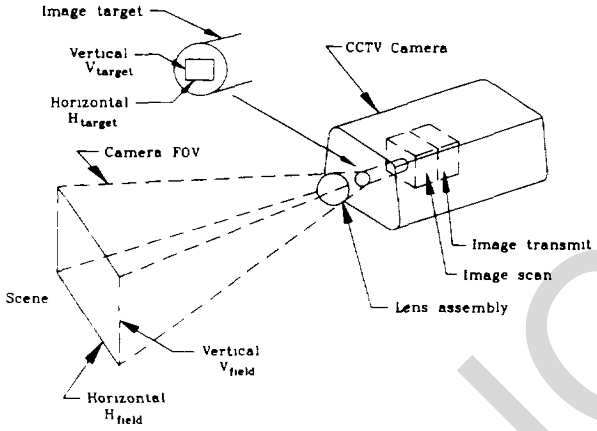


Figure 8-2 Typical CCTV Camera Components

at a remote location. Commercially available zoom lenses can accommodate changes in focal length ranging from as little as 5 to 1 to as much as 15 to 1. The ratio of maximum to minimum focal length is referred to as the magnification ratio. As might be expected, zoom lenses are at least twice the cost of fixed focal length lenses. If the zoom is to be remotely controlled, the cost will be increased further by the addition of cabling and console controls.

(2) *Diameter.* The diameter represents the maximum optical aperture through which the lens may operate and sets an upper limit on the amount of reflected light that can be captured by the lens. In practice, actual light capture will be somewhat less, because of lens reflection and transmission losses.

(3) *Adjustable aperture.* An important consideration in selecting a CCTV camera is the range of illumination which will fall on the scene to be viewed. For example, an outdoor scene in full daylight is illuminated at a level of 10,000 footcandles. On a clear moonless night, the same scene is illuminated at about 0.01 footcandle, or about a million times less light. Proper outdoor lighting is required to improve low-level illumination to about 3 footcandles. With this done, the camera has to operate over an illumination range of about 3,300 to 1. CCTV manufacturers offer a lens aperture option referred to as an "adjustable iris" to contend with wide illumination ranges. The CCTV iris acts much like the human eye's iris and is intended to maintain a constant illumination level at the faceplate of the imaging target. The iris may be adjusted either manually or automatically.

(4) *F-stop.* For a given lens focal length (fl) and aperture diameter (d), a third lens parameter, called f-stop, or lens speed, is defined by the relationship as shown in equation 8-1.

$$\text{f-stop} = \text{fl} / \text{d} \qquad \text{(eq 8-1)}$$

This dimensionless parameter is used to determine the amount of illumination available at the image target faceplate. The terms *lens speed* and *f-stop* are commonly used in photography and are associated with establishing the correct time of exposure for a photographic plate. For a focal length of 40 mm and with an aperture diameter of 10 mm, the f-stop is f/4. If the aperture diameter is increased to 20 mm, the new f-stop is f/2. Doubling the diameter quadruples the lens area, and four times the amount of light is available at the image faceplate at a stop of f/2 as compared to f/4. The adjustable iris feature controls the aperture diameter and directly controls the illumination level available at the image faceplate.

b. Image target. When the lens diameter and aperture are of proper size for the application, an image of the desired scene will lie in the focal plane of the lens system at a predictable illumination level. It is there that the faceplate of the image target is located to perform the task of converting reflected light energy to electrical impulses. A camera imaging device is specified by its format and type.

(1) *Format.* Physical size of the imaging target faceplate is specified by the camera format. Three standard sizes are commercially available: the 1-inch, the ⅔-inch, and ½-inch formats. Table 8–1 shows a comparison of physical characteristics of each format. As indicated in the table, the image area of the 1-inch format is approximately twice that of the ⅔-inch and four times that of the ½-inch. As a result, for a given lens focal length and camera location, the ⅔-inch format will contain only about half of the scene that is imaged on a 1-inch format and the ½-inch, about one fourth of the scene.

(2) *Faceplate illumination.* The amount of light energy arriving at the image faceplate is referred to as faceplate illumination and is customarily measured in footcandles. One footcandle is defined as one lumen of light flux distributed over a surface area of one square foot. A related illumination measure is the lux and is defined as one lumen distributed over a one square meter surface. A footcandle is about 10 times more intense than a lux. Faceplate illumination is dependent on the type and brightness of the source illuminating the scene, amount of reflected scene light captured by the lens, and light transmission efficiency of the lens. The relationship is defined by equation 8–2.

$$C = BTR \;/\; 4\,(\text{f-stop})^2 \qquad \text{(eq 8–2) where:}$$

C = faceplate illumination in footcandles
B = scene illumination in footcandles
T = lens transmittance efficiency (typically 0.8)
R = scene reflectivity factor

Table 8–2 displays the approximate illumination levels provided by common sources. Table 8–3 displays, as a percentage of incident light, the amount of light reflected by common surfaces.

(3) *Type.* At present, two technologies are available for fabrication of camera imaging devices. The first is based on vacuum tube technology; the second, a recent development, uses photosensitive solid-state technology. Nine types of camera imaging devices are common and commercially available. Five use the vacuum tube technol-

Table 8–1 Faceplate Dimensions 1-inch, 2/3-inch, and 1/2-inch Image Formats

Format	Vertical		Horizontal		Area Absolute		Area Relative	Aspect Ratio
inch	inch	mm	inch	mm	$inch^2$	mm^2	%	v/h
1	0.38	9.53	0.50	12.70	0.19	120.97	100	0.75
2/3	0.26	6.60	0.35	8.80	0.09	58.08	48	0.75
1/2	0.19	4.80	0.25	6.40	0.04	30.72	25	0.75

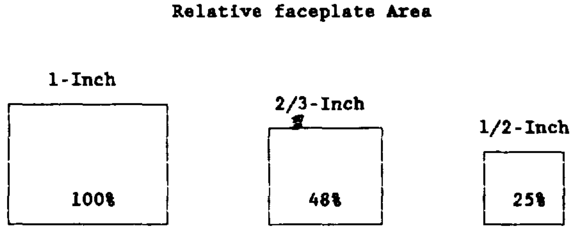


Table 8-2 Typical Illumination Ranges of Commₒn Sources

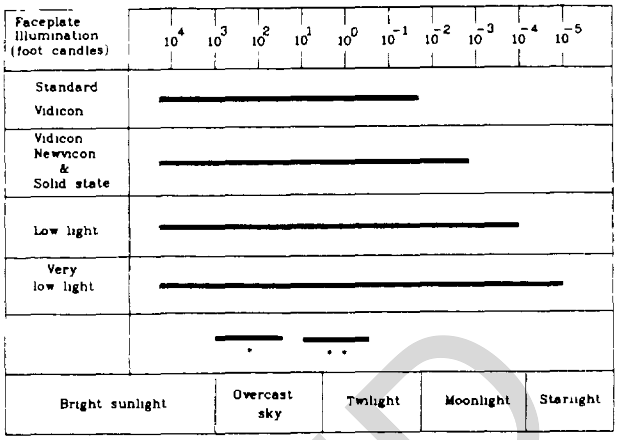
Illumination Source	Illumination Range (footcandles)
Full Sunlight	10^3 to 10^5
Indoor Lighting	0.2 x 10^1 to 10^3
Overcast Day	0 2 to 10^3
Outdoor Lighting	0.2 x 10^{-1} to 10
Twilight	10^{-2} to 0.2
Moonlight	10^{-4} to 10^{-2}
Starlight	0.2 x 10^{-7} to 10^{-4}

Table 8-3. Scene Reflectance of Common Surfaces*

Surface	Reflectance (percentage)
Empty Asphalt Surface	7
Grass-Covered Area with Trees	20
Red Brick Building	30
Unpainted Concrete Building or Surface	40
Smooth Surface Aluminum Building	65
Snow-Covered Field	75

*As a percentage of incident light

Table 8-4. Video Camera Light Range Requirements



* Typical indoor light range

* * Typical outdoor light range

ogy and four the solid-state technology. The tube types all exhibit a phenomenon called "image lag." Image lag occurs when the persistency of the photosensitive tube surface causes an object moving through the scene to appear blurred. Solid state devices do not exhibit image lag. Tube types are the vidicon, silicon-diode, zinc selenide, silicon intensifier target (SIT), and the intensified silicon intensifier target (ISIT). The solid state types are the charge-coupled device, the charge priming device, the metal oxide silicon, and charge-induced device. Of these, the charge-coupled device is the most widely used and will be discussed further. Table 8-4 presents the range of illumination levels over which the tube and solid state devices are responsive.

(*a*) *Vidicon.* The vidicon was the first imaging device used in CCTV cameras. This vacuum tube device has a phosphorescent coating to convert light energy to an electrical signal. The vidicon's spectral response is similar to that of the human eye, and requires a minimum faceplate illumination of 0.05 footcandle.

(*b*) *Low-light-level cameras.* Silicon-diode and zinc selenide cameras use image tubes with greater light sensitivity. These cameras have a wider spectral response than the vidicon. Their sensitivity extends into the infrared range and will provide a satisfactory image with about one-tenth the faceplate illumination required by the vidicon.

(*c*) *Very-low-light-level cameras.* Two classes of imaging devices are in this category: the silicon intensifier target and the intensified silicon intensifier target. Each incorporates a light amplifier ahead of the image faceplate. The intensified silicon intensifier target adds a fiber optic connection to a second image intensifier. As shown in table 8-4, these two classes of cameras can operate over the widest illumination ranges: the first from bright sunlight down to moonlight, the second from bright sunlight down to starlight.

(*d*) *Charge-coupled device.* Solid-state cameras are a recent development in CCTV camera technology. They have a broader spectral response than the human eye and response quite similar to low-light-level cameras. As shown in table 8-4, the solid state camera can operate nearly over the same illumination range as the low-light-level cameras.

c. Field of view. The scene being viewed by a camera is referred to as the camera's field of view. Important parameters are the height and width of the scene, and its distance from the camera. The field of view can be visualized as a right rectangular cone that emanates from a point perpendicular to the center of the lens. The cone is rectangular in the same proportion as the aspect ratio (width to height) of the imaging faceplate. The cone's axial length is proportional to the lens focal length, but the cone volume tends to be independent of it. As the focal length is increased, the cone grows longer, but narrower, so that the enclosed volume remains constant; then as focal length is increased, the field of view becomes deeper, but smaller. Since the field of view is imaged onto the unchanging area of the image faceplate, the scene is magnified as lens focal length is increased. The standard for relative magnification is the image captured by a 25 mm focal length lens that is assigned a magnification of 1. With this standard, a 75 mm focal length lens would provide a magnification of 3x; a 12.5 mm, 0.5x. The relative magnification is dependent only on lens focal length and is independent of format size.

d. Image target scan. This section describes image faceplate scanning and transmission to the Security Center, where it may be processed by the video processor and displayed at the console monitors as required.

(1) *Standard scan.* The standard scanning system used in the United States provides 30 complete copies of the image faceplate every second. Each copy is called a frame, but because of the human eye's persistency, the resulting sequences of frames appear as a smooth and continuous scene. A frame contains 525 horizontal scan lines but as a result of synchronization and retrace timing requirements, only 48 frame lines are available for display. A common scanning technique constructs each frame by interlacing two fields, each of which contains 50 percent of the image. The first field contains all odd numbered scan lines; the second, all even. Fields are transmitted at the rate of 60 per second and are properly phased to reconstruct the original frame on the viewing or recording device. This technique is referred to as interlace scanning. More detailed information is in EIA–330.

(2) *Composite video.* As the image faceplate is scanned, the resulting electrical signal varies according to the light level recorded for each particular point in the image. Added to this signal are synchronization pulses, used to mark the end of each scan line and each field. The signal is referred to as a "composite video signal" because it contains both scene information and signals required to interpret that information. More detailed information is in EIA–170.

(3) *Standards.* There are several standards for specifying the scanning process and composite video signal. In the United States, the frame rate is 60 per second while in Europe it is 50 per second. Once a frame rate has been selected, all CCTV components used in the system must be compatible with that rate.

8–3. Video Signal and Control Links

A CCTV transmission system is needed to convey video signals from various facility cameras to the Security Center and to carry commands from the Security Center to the cameras. Transmission may be by metallic cable, RF or optical transmission.

a. Metallic cable. Metallic video cables are electrical conductors manufactured specifically for the transmission of frequencies associated with video components. This has been the traditional method employed for CCTV. Metallic cables may have one or two center conductors, shielded by one or two concentric outer metallic braids. The cables come in three configurations: coaxial that has one inner conductor and one outer braid; triaxial that has one inner conductor and two outer braids; and twinaxial that has two inner conductors and one outer braid. The cable assembly is wrapped in an electrically insulating jacket. Special jackets are available for outdoor installations, including direct burial and rodent-resistant types. Like all electrical conductors, metallic cables will attenuate a signal in direct proportion to the length the signal travels and the frequency content of the transmitted signal. There are practical limits to cable lengths that may be used and still maintain adequate signal strength and high-frequency components. Direct cable connection between camera and monitor is limited to between 500 and 1,500 feet, depending on type of cable. If longer runs are required, video amplifier and equalization components must be interposed between the units. Also, these electrical conductors will allow ground currents to flow between locations whenever the locations experience a difference of potential like those which occur during lightning strikes. Ground currents induced in cables may interfere with the video signal and damage video equipment.

(1) *Video equalization.* Video equalization amplifiers are used to correct losses in the video signal level and high frequency attenuation, caused by long distance video transmission over metallic cables. These amplifiers usually have separate gain and equalization controls.

(2) *Ground loop correction.* Three methods are available to eliminate ground loop interference in metallic cable systems: isolation (ground loop) transformers, isolation amplifiers, or balanced twinaxial cables. Isolation transformers and amplifiers allow a metallic cable system to be referenced to earth ground at one point only so that no difference of potential can develop. Twinaxial cable confines ground current flow to a cable shield, where it cannot combine with the video signal.

(3) *Video distribution amplifiers.* A video distribution amplifier distributes multiple copies of a video signal connected to its input. The input and outputs are usually set up for 75-ohm coaxial cable connections.

b. RF transmission. For a system that has widely separated nodes, RF transmission may be an attractive alternative to metallic cable and associated amplifiers. RF transmission of several video sources can be accomplished by frequency division multiplexing of a common carrier. The multiplexed information can be transmitted over a microwave link or a broadband cable (as in commercial cable television). Broadband cable length is unlimited if repeaters are inserted about every quarter mile. A microwave link can be used for distances of about 50 miles, so long as the receiver and transmitter are in line-of-sight.

c. Optical transmission. Optical transmission of CCTV signals is a relatively new development, and two methods are in use. The first modulates a light beam and focuses the beam through air between an optic-driver-and-receiver pair. The method is less expensive than a microwave link, but its useful length is limited to about 3,000 feet and is somewhat dependent on weather conditions. The second method modulates an infrared light beam and focuses the light into a glass or plastic fiber. An optic driver and receiver are required per fiber. The fiber optic transmission method is gaining wide acceptance. It provides a low-loss, high-resolution transmission system with usable length three to ten times that of traditional metallic cable systems. Fiber optic cable is the transmission media favored by the Department of the Army.

8-4. CCTV System Sychronization

Timing signals are processed within the image scan section of the CCTV camera (see fig 8-2). These signals may be generated internally from a crystal clock, derived from the camera ac power source, or supplied by an external signal source. The camera should be capable of automatic switchover to its internal clock in the event of external signal loss. When CCTV cameras are supplied by a common external (master) signal source, or are all powered from the same ac power source, all cameras scan in synchronism. In this case, a console CCTV monitor will display a smooth transition when switched from one video source to another. Without this feature, the monitor display breaks-up or rolls when switched between video sources. The rolling occurs for as long as it takes the monitor to synchronize its scan with that of the new video source, typically one second. The resynchronization delay will be experienced by all system components that receive video information, including recorders. To avoid this delay, the designer must specify that all cameras are powered from the same AC power phase or must specify master synchronization for the design.

8-5. Video Processing and Display Components

As depicted in figure 8-1, CCTV camera signals propagate through the video transmission system and converge at the security center. In very simple configurations with only a few cameras and monitors, a hard-wired connection between each camera and console monitor is adequate. As the number of cameras increases, the need to manage and add supplemental information to camera signals also increases. Psychological testing has demonstrated that the efficiency of console operator assessment improves as the number of console monitors is reduced, with the optimum number being four to six monitors. Effectiveness is also enhanced by the use of alarm correlated video. Major components of the video processor system are the video switcher, video loss detector, alarm processor communication path, master video sync generator, video recorders, and monitors.

a. Video switchers. Video switchers are required when the number of cameras exceeds the number of console monitors or when a monitor must be capable of selecting video from one of many sources. Switchers are classified as either active or passive and are available with a wide spectrum of features. The simplest ones are manually controlled, mechanical (passive) type and are adequate for small surveillance systems. They are not useful in a rapid alarm assessment environment. Switchers have been evolving, and they have benefitted, like many other devices, from the advent of solid state electronics, including microprocessor based controllers. A CCTV switcher can be implemented by using one central switcher or several remote switchers connected to a central switcher. An example of each arrangement is diagrammed in figure 8-3. The use of remote switchers can reduce the number of video transmission links routed to the Security Center; however, an additional data link is necessary to control the remote switchers. For perimeter alarm assessment, environmental protection for the remote switcher is required. These devices are designed for controlled interior conditions and cannot be used in extreme temperatures or other adverse situations. When considering the use of remote switchers, the designer must perform a cost analysis to determine whether or not they offer a real cost savings. An appropriate alarm assessment switcher includes the following features:

(1) Compatible with EIA-170 specifications.

(2) Active, all solid state computer based operation.

(3) Operator programmable at the console.

(4) Modular construction to support expansion and maintenance.

(5) Alarm processor operator override during IDS alarms.

(6) On/off recorder control capability during IDS alarms.

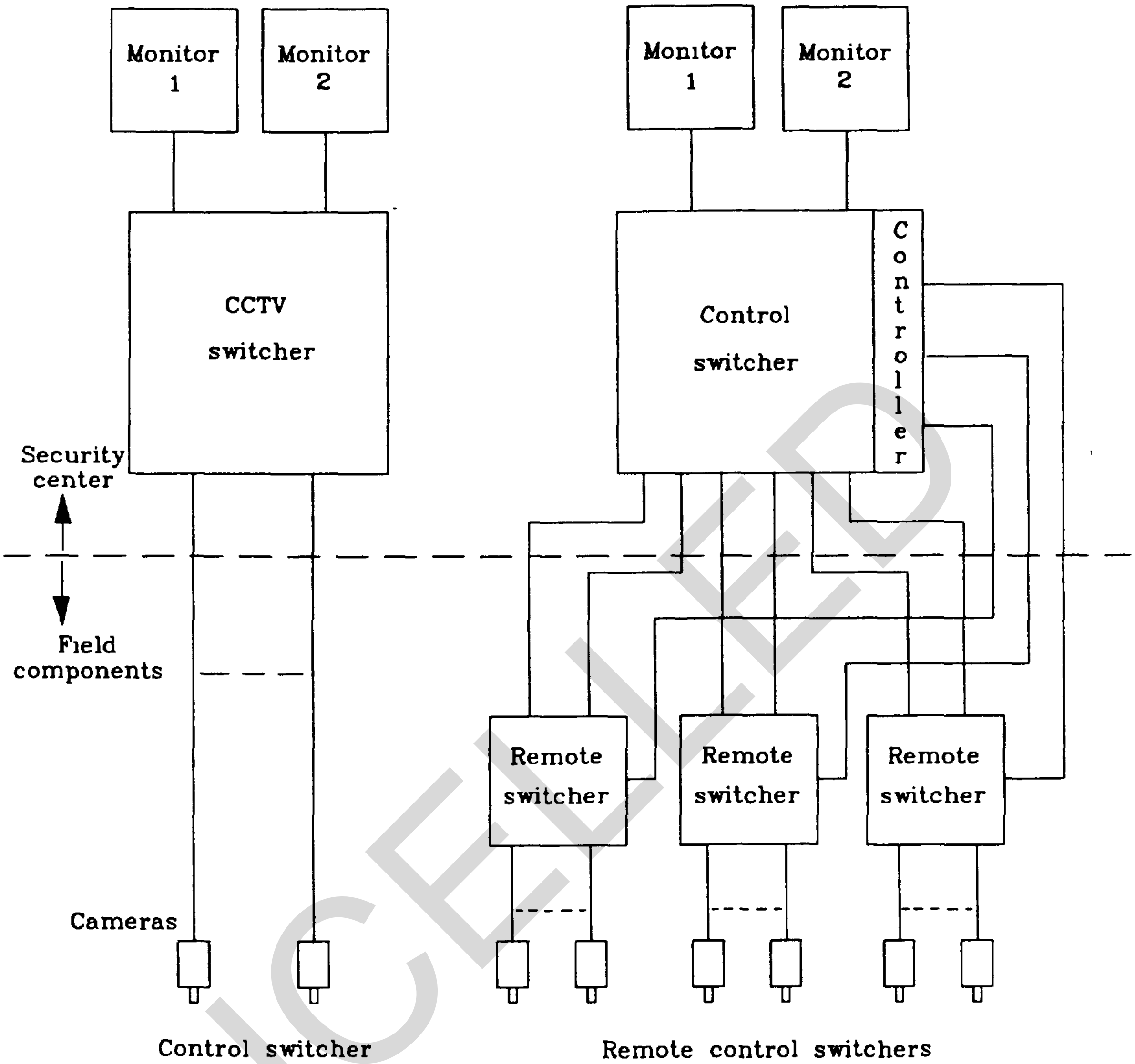


Figure 8-3. CCTV Switcher Arrangements.

(7) Settable clock, calendar, and zone information appended to composite video output signals.

b. Video loss detector. Video loss detectors sense the continued integrity of incoming camera signals. They should be installed on each incoming video signal whenever a switcher is used. When a camera signal fails or is otherwise interrupted at the video switcher input, a signal is sent to the alarm processor. In a properly designed system, this signal is annunciated to the console operator to indicate that a portion of the assessment system has become unavailable. Video loss detectors should incorporate the video-loop-through feature. Loop-through ensures the camera signal continues to appear at the switcher input should the loss detector fail.

c. IDS interface and communication path. There must be a means of rapid communication between the IDS alarm annunciation and video processor systems. The alarm processor must send commands that cause the video switcher to select the camera appropriate for the sensor reporting an alarm. The video processor system must report system tampering or failures, such as loss of video, to the alarm processor. The path should also pass date and time synchronizing information between processors so that recorded video scenes and printed alarm logs are properly correlated.

d. Master sync generation and distribution. Master video sync includes a crystal controlled timing generator, distribution amplifiers, and a transmission link to each camera. The generator supplies the scan timing signals to the distribution amplifiers. The amplifiers drive transmission links so that each camera receives an in-sync replica of the timing generator output.

e. Video recorders. Video recorders provide means to record alarm event scenes in real-time for later analysis. A recorder typically receives its input through dedicated video switcher outputs. To support recorder playback, the recorder output is connected to a dedicated switcher input and must be compatible with the switcher signal format. In addition, the recorder receives start commands from the switcher, and compatibility must also exist at this interface. Video recorders are available that provide either continuous or single frame recording. Single frame recorders will be used when a video frame is sufficient to record an alarm event. Continuous recorders will be used when alarm events are to be recorded for later playback and analysis.

(1) *Continuous recorders.* Traditionally, continuous recorders have been reel-to-reel magnetic tape type. The video cassette recorder has now replaced reel-to-reel types in most security applications. The cassettes can record in time lapse for up to 240 hours, depending upon the user-selected speed, and will change to real-time recording upon command. The cassettes can be erased and reused or archived if required. Continuous recorders store information serially; that is, the media can be indexed to a particular stored scene only by moving forward or backward from its present location.

(2) *Single frame recorders.* Single frame recorders are available in either hard disk or solid-state semiconductor array packages.

(*a*) *Hard disk.* The hard disk has the capacity to store several thousand video frames. It is a random access device so that a particular frame can be called-up for display in a fraction of second. This device is usually controlled by a microprocessor imbedded as part of the recorder package or as a peripheral to the video processor computer.

(*b*) *Semiconductor array.* Semiconductor arrays are the fastest devices available for storage of single frame scenes. They require very little host system support but are limited to storing a few frames. The array storage is volatile, meaning that images can be retained only so long as the device remains powered. The video information can be removed and archived only by downloading to a nonvolatile recording device. The devices are relatively new and already experiencing price reductions.

f. Monitors. Monitors are required to display the individual scenes transmitted from the cameras or from the video switcher. In alarm assessment applications, the monitors are driven by dedicated outputs of the video switcher and the monitors display video sources selected by the switcher. Moderately priced units displaying 625 scan lines with a video bandpass of 7 MHz are common. Higher resolution units are available at higher cost. The number of shades of gray a monitor can display is called the monitor's "gray scale capability." Monitors with at least 10 discernible shades of gray will be specified. The diagonal measure of the monitor viewing surface is used to specify its nominal size, which can be from 5 to 36 inches. For security console operations, the 9-inch monitor is the smallest screen that should be used for operator recognition of small objects in a camera's field of view. Two such 9-inch monitors can be housed side by side in a standard 19-inch console. If the monitors are to be mounted in free-standing racks behind the security console, larger units will be used.

g. Video annotation Video processor equipment will be specified to append the following alphanumeric information so it appears on both monitors and recordings. The equipment must allow the operator to program the annotated information and dictate its position on the screen.

(1) Time and date information.

(2) Video source or alarm zone identification.

(3) Programmable titles.

Section II. APPLICATION GUIDELINES

8-6. Site Specific Factors

Site-specific factors must be taken into consideration in selecting components that comprise a particular CCTV system. The first is the system size in terms of the number of cameras fielded, which is the minimum number needed to view all IDS sensor detection fields. Another factor is the maximum anticipated alarm rate, which may require that the video processor system record CCTV scenes for later playback during operator assessment. Another factor is that artificial light sources may be required by some CCTV cameras. Finally, there are CCTV system performance criteria, physical and environmental considerations, and economic considerations. Each is discussed in this section.

8-7. Performance Criteria

a. Scene resolution. The level to which video details can be determined in a CCTV scene is referred to as resolving ability or resolution. It is generally accepted that for assessment purposes, three resolution requirements can be defined. In order of increasing resolution requirement they are detection, recognition, and identification. Detection is the ability to detect the presence of an object in a CCTV scene. Recognition is the ability to determine the type of object in a CCTV scene (animal, blowing debris, or crawling human). Identification is the ability to determine object details (a particular person, a large rabbit, a small deer, a tumbleweed). A CCTV assessment system should provide sufficient resolution to recognize human presence and to detect small animals or blowing debris. Given an alarmed intrusion sensor, it is crucial that the console operator be able to determine if the sensor detected an intruder or is simply responding to a nuisance condition.

(1) *Video line resolution.* Video resolution is specified for horizontal as well as vertical directions. Horizontal resolution is specified as the maximum number of alternating light and dark vertical lines that can be distinguished in the display; vertical resolution is specified as the maximum number of alternating light and dark horizontal lines that can be distinguished. For adequate resolution (recognition), an object should occupy no less than five horizontal scan lines. This five-line resolution requirement is a system-wide requirement imposed on cameras, video cabling, processors, and monitors. A system specified at 525 scan lines, with 5 MHz vertical bandpass, will provide adequate resolution for most assessment CCTV applications. Higher resolution systems are available for assessment functions that require object identification but at considerably higher cost.

(2) *Focal length resolution limits.* Because of synchronization and timing requirements, only 485 horizontal scan lines in a 525 scan line system can be displayed. To determine the object size that will occupy five horizontal scan lines at a given distance, it is necessary to calculate the vertical field of view at the given distance, for a particular lens focal length. This dimension is then multiplied by the factor 5/485. The required minimum video bandpass that will provide equivalent horizontal resolution can also be determined. Because of the image aspect ratio (vertical / horizontal = 0.75), a 525 horizontal scan line system would require 650 vertical lines (485 / 0.75). A 650 vertical line resolution is equivalent to a minimum video bandpass requirement of 5 MHz. Therefore, given a target size and scan line resolution requirement, a table displaying the maximum distance at which the specified target will be recognized can be generated. The table columns should be organized by lens focal length. The generally accepted criteria for small object resolution is that a 7.5-horizontal-inch object (the size of a small animal) should occupy no less than 0.75 percent of the horizontal field of view. With this criteria, a simple calculation defines the maximum horizontal field of view dimension as 83 feet. Table 8-5 presents, for some commonly used focal lengths, the maximum distance at which a 7.5-inch object is recognizable. Even though the object may occupy the required number of scan lines, a console operator is still dependent on the object's contrast with the background and is interrelated with scene lighting, background color, and object movement.

Table 8-5 Maximum Distance at Which a 7 5-inch Object May Be Recognized.

Lens Focal Length	(mm)	6.5	12.5	25	37.5	50	75	100	150
Distance From Camera	* (ft)	59	118	236	354	472	707	943	1415

* Distance is computed by using the standard criteria·
- the object must occupy at least 0.75% of the horizontal Field-Of-View.

The following must also be true
- the object contrasts with the scene background,
- reflected scene light at the image faceplate is within proper range,
- the CCTV system is capable of 650 vertical line resolution

(3) *Depth-of-field.* A third consideration associated with scene resolution is depth of field. Depth of field quantifies the range of objects that will be in focus as one moves away from the camera toward the background. Depth of field will increase (more of the near and distant objects will be in focus) as the f-number increases. This is because, as the f-number is increased, less lens edge area is used to cast the scene image onto the faceplate. Light rays diffracted through the center of the lens (larger radius of curvature) are bent through a smaller angle than rays at the edges (smaller radius of curvature). As the radius of curvature increases, so does depth of field. For CCTV systems, where objects must be in focus over a wide depth of field, the CCTV and lighting system must be designed so that low f-numbers (full lens openings) are not required under normal operating conditions. Another good practice is to use a lens format that is one size larger than the camera faceplate format. Depth of field will be improved, for example, if a 1-inch lens is used with a ⅔-inch faceplate or a ⅔-inch lens is used with a ½-inch faceplate, but remember, field of view calculations are always based on faceplate format and lens focal length.

b. Response time. The time lapse between an IDS sensor going to the alarm state and the time it takes to present the console operator with a specific scene containing that sensor's detection field is known as the assessment start delay time. That portion of delay directly attributable to the video processor system is the time lapse between receipt of the video source select command from the alarm processor and presentation of the selected scene to the console operator and video recorders. It is reasonable to expect commercially available switchers to respond in one-frame time (1/30th of a second) or less. For perimeter alarm assessment, the designer must specify system components that will assure that the assessment start delay time is less than one second. Video cassette recorders may require an additional second to accelerate the tape to recording speed; if not acceptable, consider fast response single frame recorders.

8-8. Lighting and Imaging Considerations

a. Illumination levels. For interior applications, where the same camera type is to be used in several different areas, and scene illumination in each area is constant, specify the manually adjustable iris. This allows a manual iris adjustment appropriate for each particular area illumination level at the time of installation. If the camera must operate in an area subject to a wide dynamic range of illumination levels, specify the automatically adjusted iris feature.

b. Selecting the imaging target type. Select the imaging target type on the basis of illumination source and the range of illumination levels with which the camera must operate. Figure 8-4 displays the spectral response typical for the imaging types discussed. The figure also displays spectral output produced by some common illumination sources demonstrating that the spectrum produced by a sodium vapor lamp would not be a good illumination source for very low light level cameras (intensifiers).

(1) *The vidicon.* Use the vidicon for daylight or well-lighted interiors. The faceplate is subject to long term burn-in, which means that, if the vidicon views a fixed scene, the scene will, in time, become permanently recorded in the phosphorescent coating. If the vidicon is subjected to an inadvertent bright spot, such as a searchlight, the image may be permanently burned into the phosphor. The standard vidicon is least expensive but has a shorter service life than the CCD camera.

(2) *Low light level cameras.* These cameras can provide an acceptable image with as little natural illumination as provided by dusk conditions. Because of the wide dynamic range over which these cameras may operate, they are available with auto-iris and optional automatic light control. Low light level cameras are not damaged by an inadvertent bright spot, nor are they subject to fixed image burn-in. Low light level cameras cost about four times as much as a standard vidicon.

(3) *Very low light level cameras.* As shown in table 8-4, these cameras can operate over the widest illumination ranges, from bright sunlight down to starlight. To accommodate this wide range, very low light level cameras should be equipped with one or more forms of light control, such as automatic iris control, neutral density filters, or automatic gain control. These cameras have poor resolution, are subject to fixed image burn-in, and will lose image contrast if a bright light source suddenly appears in the field of view. Very low light level cameras cost about ten times as much as a standard vidicon depending on options. These cameras have a relatively short service life.

(4) *Charge-coupled device.* The charge-coupled device is inherently more rugged and reliable than vacuum tube types, is not subject to burn-in problems, has a longer service life, and can be packaged in a smaller volume. These cameras are moderately priced and are finding wide acceptance in security applications.

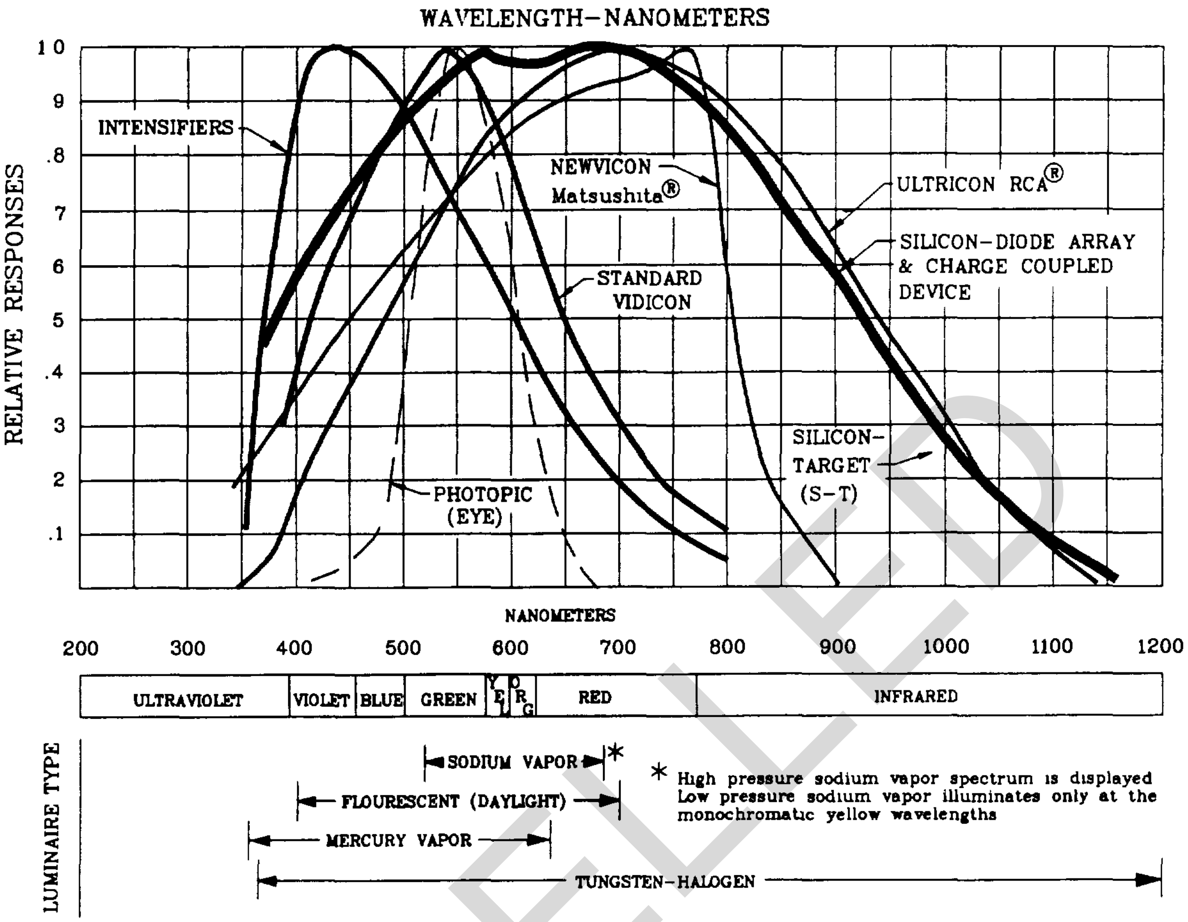


Figure 8-4 Spectral Response

c. Lens and format selection. Once the designer has determined the scene's height, width, and distance from the camera, as well as the illumination levels under which the camera must operate, an appropriate camera format, lens, and imaging type can be selected. Standard lens tables are widely available. Tables are organized by image format: 1-inch or ⅔-inch or ½-inch. For a given format, table rows are usually indexed by increasing value of lens focal length, with the columns arranged by increasing distance from the camera. Located at each row and column intersection is the maximum scene height and width that can be observed. Maximum resolution is maintained by selecting the shortest focal length lens that will accommodate the required scene height and width. Table 8-6 is a lens selection table based on the 1-inch image format; table 8-7 is based on the ⅔-inch image format; and table 8-8 is based on the ½-inch image format. As indicated in table 8-1, the ½-inch format will image only about 25 percent of the area of the 1-inch format and about 50 percent of the area of the ⅔-inch format. The designer must determine scene resolution requirements carefully when selecting image format size for a particular site. In general, CCTV resolution requirements for alarm assessment can be met by ½-inch image format cameras. Where higher resolution is required, such as when the console operator must be able to determine what a person approaching a building is carrying, the designer will consider a larger image format.

8-9. Economic Considerations

Cost of a CCTV system is usually quoted as cost per assessment zone. When estimating total system cost, video processor equipment costs and the video transmission system costs must be included. Other potentially significant costs are outdoor lighting system upgrades and site preparation required to support the CCTV cameras. CCTV systems are expensive compared to other electronic security subsystems and should be specified with discretion. Regardless of cost, they are an essential part of a large exterior system unless the entire area is under constant visual observation, such as by guards in towers. In some instances, assessment CCTV will be dictated by regulation, value of the asset, or remoteness of the protected areas.

Table 8-6. Lens Selection Table: 1-inch Format

1-inch format																		
Lens	Angular Field-of-View		Distance From Camera to Scene (ft)															
Focal Lngth	Vert	Horiz	10		20		50		100		150		200		300		400	
			Dimensions of the Field of View at that distance (ft)															
(mm)	(deg)	(deg)	V	x H	V	x H	V	x H	V	x H	V	x H	V	x H	V	x H	V	x H
4.0	99.9	115.6	23.8	31.8	47.6	63.5												
6.5	72.5	88.7	14.7	19.5	29.3	39.1	73.3	97.7										
8.5	58.5	73.5	11.2	14.9	22.4	29.9	56.0	74.7										
12.5	41.7	53.9	7.6	10.2	15.2	20.3	38.1	50.8	76.2	101.6								
25.0	21.6	28.5	3.8	5.1	7.6	10.2	19.1	25.4	38.1	50.8	57.2	76.2	76.2	101.6				
37.5	14.5	19.2	2.5	3.4	5.1	6.8	12.7	16.9	25.4	33.9	38.1	50.8	50.8	67.7	76.2	101.6		
50.0	10.9	14.5	1.9	2.5	3.8	5.1	9.5	12.7	19.1	25.4	28.6	38.1	38.1	50.8	57.2	76.2	76.2	101.6
75.0	7.3	9.7	1.3	1.7	2.5	3.4	6.4	8.5	12.7	16.9	19.1	25.4	25.4	33.9	38.1	50.8	50.8	67.7
100.0	5.5	7.3	1.0	1.3	1.9	2.5	4.8	6.4	9.5	12.7	14.3	19.1	19.1	25.4	28.6	38.1	38.1	50.8

Table 8-7. Lens Selection Table: ⅔-inch Format

2/3-inch format																		
Lens	Angular Field-of-View		Distance From Camera to Scene (ft)															
Focal Lngth	Vert	Horiz	10		20		50		100		150		200		300		400	
			Dimensions of the Field of View at that distance (ft)															
(mm)	(deg)	(deg)	V x H		V x H		V x H		V x H		V x H		V x H		V x H		V x H	
4.0	79.1	96.0	16.5	22.2	33.0	44.4												
6.5	53.9	68.7	10.2	13.7	20.3	27.4	50.8	68.4										
8.5	42.5	55.2	7.8	10.5	15.5	20.9	38.8	52.3										
12.5	29.6	39.2	5.3	7.1	10.6	14.2	26.4	35.6	52.8	71.1								
25.0	15.0	20.2	2.6	3.6	5.3	7.1	13.2	17.8	26.4	35.6	39.6	53.3	52.8	71.1				
37.5	10.1	13.5	1.8	2.4	3.5	4.7	8.8	11.9	17.6	23.7	26.4	35.6	35.2	47.4	52.8	71.1		
50.0	7.6	10.2	1.3	1.8	2.6	3.6	6.6	8.9	13.2	17.8	19.8	26.7	26.4	35.6	39.6	53.3	52.8	71.1
75.0	5.0	6.8	0.9	1.2	1.8	2.4	4.4	5.9	8.8	11.9	13.2	17.8	17.6	23.7	26.4	35.6	35.2	47.4
100.0	3.8	5.1	0.7	0.9	1.3	1.8	3.3	4.4	6.6	8.9	9.9	13.3	13.2	17.8	19.8	26.7	26.4	35.6

Table 8-8. Lens Selection Table: ½-inch Format

1/2-inch format																		
Lens	Angular Field-of-View		Distance From Camera to Scene (ft)															
Focal Lngth	Vert	Horiz	10		20		50		100		150		200		300		400	
			Dimensions of the Field of View at that distance (ft)															
(mm)	(deg)	(deg)	V x H		V x H		V x H		V x H		V x H		V x H		V x H		V x H	
4.0	62.2	76.9	12.1	15.9	24.1	31.7												
6.5	40.7	52.1	7.4	9.8	14.8	19.5	37.1	48.8										
8.5	31.7	41.0	5.7	7.5	11.4	14.9	28.4	37.4										
12.5	21.9	28.5	3.9	5.1	7.7	10.2	19.3	25.4	38.6	50.8								
25.0	11.0	14.5	1.9	2.5	3.9	5.1	9.7	12.7	19.3	25.4	29.0	38.1	38.6	50.8				
37.5	7.4	9.7	1.3	1.7	2.6	3.4	6.4	8.5	12.9	16.9	19.3	25.4	25.7	33.9	38.6	50.8		
50.0	5.5	7.3	1.0	1.3	1.9	2.5	4.8	6.4	9.7	12.7	14.5	19.1	19.3	25.4	29.0	38.1	38.6	50.8
75.0	3.7	4.8	0.6	0.8	1.3	1.7	3.2	4.2	6.4	8.5	9.7	12.7	12.9	16.9	19.3	25.4	25.7	33.9
100.0	2.8	3.6	0.5	0.6	1.0	1.3	2.4	3.2	4.8	6.4	7.2	9.5	9.7	12.7	14.5	19.0	19.3	25.4

Section III. DESIGN GUIDELINES

8–10. System Familiarity

Before designing an effective CCTV assessment system, the designer must be familiar with IDS sensor placement and detection field shape.

8–11. CCTV Camera Placement and Lighting

This section provides guidance for placement of exterior and interior cameras. Placement of exterior cameras requires more attention than placement of interior cameras because of weather and illumination extremes.

a. General guidelines.

(1) *Field of view alignment.* The optimal CCTV/alarm assessment design occurs when each camera includes an entire intrusion sensor detection field within its field of view. This is not to say that each intrusion sensor must have its own camera; several sensor detection fields may be within the field of view of the same camera, or if site conditions dictate, an IDS zone may require two or three cameras to provide adequate coverage. If multiple cameras are required for any IDS zone, then the video system specified must be capable of simultaneously displaying all cameras associated with that zone. Typically, a single CCTV camera will assess a single perimeter IDS zone. Each IDS zone may include several types of alarm sensors such as fence disturbance and volumetric. If the detection field follows uneven terrain, several cameras may be needed to view the entire detection zone and the interface between the alarm processor and video processor systems will be more complex.

(2) *Illumination range.* The designer will minimize the illumination range over which assessment cameras must operate.

(*a*) *Visible light sources.* In electronic security systems, most frequently used light sources are those that produce light energy in the visible frequency ranges. The frequency spectrum produced by these sources is depicted in figure 8–4.

(*b*) *Invisible light sources.* Using visible light sources to illuminate a perimeter and outdoor areas provides an obvious night-time signature to intruders. The perimeter may be located in proximity to a civilian area, where use of visible spectrum night-lighting may be objectionable. As an alternative, spectrally matched infrared lighting and cameras are available. Referring to figure 8–4, the tungsten-halogen family provides usable light energy well into the infrared range. With the visible light energy absorbed by filters, silicon-diode and solid state cameras will provide satisfactory images in the infrared spectrum. The response force will require night vision equipment to gain a tactical advantage over an intruder.

(3) *Balanced lighting.* The best image contrast is obtained by a scene that is uniformly illuminated. Table 8–4 lists minimum faceplate illumination required by the common imaging devices now available. These values can be read at the right side of each range line. The table indicates that all imaging devices can operate with as little illumination as that available at twilight. As the average light energy reaching the image faceplate approaches the minimum required, the image produced will have proportionally reduced contrast and become washed out. This may not be a serious disadvantage for CCTV surveillance. However, if the cameras are required to support rapid operator assessment of IDS alarms, high contrast video should be provided. The designer should consider artificial lighting, uniformly applied, to raise the minimum light energy reaching the image faceplate. A CCTV outdoor lighting system should illuminate the camera field of view so that the maximum light to dark ratio does not exceed six, while providing a minimum illumination level of two foot-candles throughout the assessment area.

(4) *Camera and light source alignment.* The camera must be located below the plane of lighting fixtures used to illuminate the area. If side lighting is used, the camera should not look directly into the lighting plane. The lighting fixtures and cameras should be aimed in the same direction.

b. Indoor considerations.

(1) *General.* Interior intrusion sensors require alarm assessment whenever the sensors are placed in "secure" mode. This is usually during off-hours for heavily trafficked areas or continuously for storage areas.

(2) *Mounting location.* Cameras should be mounted at a height that reasonably precludes accidental damage by collision during normal area operations. Select a location that will preclude inadvertent blockage of the camera's field of view and which will allow the camera to be connected to the power and video transmission systems.

(3) *Tamper detection.* When the selected camera mounting location will subject the camera to possible tampering, the designer will include tamper detection and reporting capability in the design.

c. Outdoor considerations.

(1) *Housing.* A camera located outdoors requires protection from the elements, which can be provided by an environmentally sealed housing. The housing should be charged with dry nitrogen

to prevent condensation from forming inside the camera. A thermostatically controlled heater, sunshield, window defroster, and tamper-alarmed enclosure will also be specified for the housing as appropriate.

(2) *Mounting/mast.* Outdoor camera mountings must provide a stable base to support camera and housing during high winds. A CCTV camera that is to provide perimeter alarm assessment will usually be mounted on a mast and use a lens of relatively long focal length. Wind and ice load effects will be considered when selecting an outdoor mount/mast.

(3) *Mounting/mast location.* Alarm assessment cameras will be located within protected areas in positions of minimal vulnerability. As an example, perimeter camera masts will typically be located inside the perimeter/isolation zone and within the detection field of one or more perimeter IDS alarm sensors.

(4) *Camera compass bearing.* When a choice about directing the camera field of view is available, choose the direction that will avoid viewing the rising or setting sun.

8-12. Layout Considerations

Camera field of view and sensor detection fields will be aligned so that an alarm sensor can be assessed by a specific camera when possible.

a. Perimeter zone alignment. The perimeter IDS design will consider clear zone width and length in determining camera placement.

(1) *Clear zone width.* A typical perimeter IDS will include a clear zone created by inner and outer fencing that encloses the area to be protected. Distance between these fences and elevation of cameras will determine the setback distance for each perimeter camera. The setback distance will be selected to ensure that the camera field of view includes the full clear zone width at ground level throughout the IDS zone.

(2) *Clear zone length.* The nominal length of a perimeter zone may be dependent upon the perimeter terrain.

(*a*) *Flat terrain.* If the perimeter is basically flat, the perimeter zone length will be determined by CCTV object recognition requirements within the zone.

(*b*) *Undulating terrain.* If the perimeter includes crests and valleys to the extent that cut-and-fill earth moving operations would be cost prohibitive, the perimeter zone lengths will be based on sensor and camera layouts that preclude the presence of terrain "blind spots" that would allow an intruder to use crouching or crawling movements to avoid detection and assessment.

b. Indoor considerations. The layout for indoor alarm assessment cameras is subject to three constraints:

(1) The camera location should enclose the complete sensor(s) detection field in the camera's field of view.

(2) Lighting adequate to support alarm assessment will be provided.

(3) Protection from tampering and inadvertent damage by collision during normal area operations will be provided.

8-13. Camera Placement Procedure and Formulas

The following design procedure will be used to determine correct CCTV camera placement. The most critical placement problem is to locate a camera so that its field of view aligns properly with an outdoor perimeter detection zone. If this process is understood, other less demanding applications will also be understood.

a. Define parameters. To begin the design, certain parameters of the IDS perimeter must be determined by the designer.

(1) *Control zone width.* The protected perimeter is normally constructed of two fences, an inner and an outer. The perpendicular distance between the two fences is called the *zone width* (ZW). The camera will be located so that at the beginning of the zone the entire zone width is included in the camera's field of view. This parameter is referred to as the camera's setback distance.

(2) *Resolution required at end of zone.* CCTV scene resolution requirements determine the width of the field of view required at the far end of the zone (WZE). This parameter is required to determine the maximum distance a camera may be located from the far end of its zone.

(3) *Camera height.* The CCTV camera will usually be mounted above the scene to be viewed. The amount of vertical offset (VO) used to position the camera will influence both the setback and vertical tilt dimensions of camera placement.

(4) *Vertical scene height at end of field.* This parameter identifies the scene height that must be included in the camera field of view at the end of the detection zone (VZE). For example, if perimeter fencing extends 7 feet above grade, the designer may choose 9 feet as the minimum height to be displayed at the far end of the zone. This allows a 2-foot view above the fence top at the far end of the zone, which is sufficient to see an intruder at the fence top.

(5) *Required zone length.* This parameter identifies the detection zone length to be included in the camera's field of view.

b. Design procedure. Given the preceding parameters, the camera placement calculations will follow the steps to be described.

(1) Choose the image format size. The designer will choose a camera image format size, defining the image target horizontal (Ht) and vertical (Vt) dimensions. Dimensions for the 1-, ⅔-, and ½-inch formats are as shown in table 8–1.

(2) Choose a lens focal length. With the image format size and focal length (fl) selected, the horizontal and vertical lens opening angles can be calculated using the following formulas from equation 8–3 and 8–4.

Horizontal opening angle (ih):

$$ih = 2 * \text{arc tan } (Ht / (2 * fl)) \qquad \text{(eq 8–3)}$$

Vertical opening angle (iv):

$$iv = 2 * \text{arc tan } (Vt / (2 * fl)) \qquad \text{(eq 8–4)}$$

The designer is cautioned that Ht, Vt, and fl must be specified in consistent units, usually millimeters. Tables 8–6 through 8–8 tabulate the lens opening angles for some common lens focal lengths. The tables are organized by lens format sizes of 1-, ⅔-, and ½-inch respectively. The tables include horizontal and vertical field of view dimensions at selected distances from the camera.

(3) Calculate maximum distance to end-of-zone. Using the horizontal lens opening angle (ih) and the minimum width required at the far end of zone (WZE), the designer will calculate the maximum acceptable distance (MD) between camera and the far end-of-zone as shown in equation 8–5.

Maximum Distance to end-of-zone (MD):

$$MD = (WZE/2) / (\tan (ih / 2)) \qquad \text{(eq 8–5)}$$

Where MD is specified in the same units as WZE:

(4) Calculate the camera tilt angle. Given a required end-of-zone minimum height (VZE) and camera mast height (VO), the camera will require some vertical tilt towards the ground. This angle (it) is given by equation 8–6.

$$it = \text{arc tan } ((VO–VZE) / MD) + iv/2 \qquad \text{(eq 8–6)}$$

The designer will note that as the lens focal length is increased the required tilt angle decreases. The formula assumes level terrain, so if the terrain has a gradual slope (positive or negative), a small field adjustment will probably be required.

(5) Calculate distance to ground strike. Given the camera mast height (VO), calculated lens vertical opening angle (iv), and camera tilt angle (it), the distance at which the camera field of view first strikes the ground (GS) may be calculated using equation 8–7.

$$GS = VO / \tan (it + iv/2) \qquad \text{(eq 8–7)}$$

(6) Calculate the camera setback distance. With the zone width (ZW) specified, the distance at which the camera must be set back (the distance ahead of the beginning of the zone, SB) is calculated using equation 8–8.

$$SB = ZW / (2 * \tan (ih/2)) \qquad \text{(eq 8–8)}$$

Note that SB is specified in the same units as is ZW, usually in feet.

(7) Calculate the available zone length. The available zone length (AZL) is defined as the maximum distance that will yield system resolution requirements (usually small object resolution) minus the camera setback distance (SB) required to present the full control zone ground level view at the zone's beginning. The expression is given shown in equation 8–9.

$$AZL = MD - SB \qquad \text{(eq 8–9)}$$

If the calculated available zone length is shorter than the specified zone length, a longer focal length lens should be selected and the procedure repeated. Conversely, if the available zone length is much longer than required, a shorter focal length should be selected and the procedure repeated.

c. Procedure summary. As an example, table 8–9 summarizes concepts presented in this section by solving a specific set of design input parameters. The table tabulates the resulting field of view parameters for several common lens focal lengths. For a 200 foot zone length, the table indicates that a 35-mm lens would be best suited (AZL = 210.8 feet). The camera would be set back at least 119 feet but no more than 130 (to meet the 200-foot zone length requirement). The camera would be tilted about 6 degrees towards the ground. The first sight of ground or ground strike will occur 72 feet downstream of the camera location (centered at the bottom of the CCTV screen). Full view of the ground (zone width) will occur at 119 feet. The top of a 9-foot object, at the far end of the zone, will occupy the top-most scan-lines. In this example, the following design inputs are used:

(1) A camera mast height of 15 feet.

(2) A control zone width of 30 feet.

(3) A resolution requirement that an object 7.5 inches wide occupy at least 0.75 percent of the horizontal line.

(4) A vertical height of 9 feet will be visible in the far end field of view.

(*a*) *General applications.* The designer will use the formulas presented in this section to test understanding of terms and concepts presented. The resulting calculations should agree with those in table 8-9. With that accomplished, it is easy to create new tables for other applications. The procedure can be easily adapted for spreadsheet solution using a desktop or personal computer.

(*b*) *Graphic aids.* As a further design aid, the camera layout parameters calculated can be used to construct transparent templates. The templates can be used to graphically depict the camera horizontal field of view (horizontal opening angle) when overlaid on a plan (top-down) view of the zone. Arc lines can be added that indicate where ground-strike (GS), full zone width (SB), and maximum resolution distance (MD) occur in the field of view. Each template will be unique to the specified design input parameters and image format size, and each focal length will require a separate template. The procedure and template both assume constant slope terrain between the camera and the far end of the zone, and adjustments will be necessary if this is not the case.

8-14. CCTV System Interfaces

In designing an alarm assessment CCTV system, certain interfaces will be required if an acceptable system is to result.

a. Alarm assessment lighting system. When possible, the lighting system and CCTV system will be designed concurrently. The designer will coordinate the need for adequate lighting of uniform intensity and compatible spectral output (see video camera light range comparisons in the table 8-4). In the case of existing lighting systems, light measurements will be taken to determine if lighting upgrades are required. A CCTV outdoor lighting system must illuminate the camera field of view so that the maximum light-to-dark ratio does not exceed 6, while providing a minimum illumination level of 2 foot-candles throughout the assessment area.

b. Security center. The CCTV system designer will locate cameras throughout the facility where required and locate video processor equipment and monitors at the Security Center.

(1) *Console space.* Space will be provided in the control console for CCTV monitors to be at operator eye-level. Depending on IDS size, two to

Table 8-9. Camera Placement Calculations: ⅔-inch Format

Design Input Parameters:

Zone Width	ZW	30 ft	
Max Width @ end of Zone	WZE	83 ft	(7.5-inch is 0.75% of horiz.)
Camera Vertical Offset	VO	15 ft	
Min. height @ end of Zone	VZE	9 ft	

Ht = 8.8 mm
Vt = 6 6 mm

Lens Focal Length fl	Oh	Ov	Distance to Min. Res. MD	Camera Tilt Ot	Ground Strike GS	Camera Setback SB	Avail. Zone Length AZL
(mm)	(deg)	(deg)	(ft)	(deg)	(ft)	(ft)	(ft)
6 25	70.3	55.7	58.9	33.6	8.2	21.3	37.6
12.50	38.8	29.6	117.9	17.7	23.6	42.6	75.3
25.00	20.0	15.0	235.8	9.0	50.6	85.2	150.6
35.00	14.3	10.8	330.1	6.4	71.7	119.3	210.8
37.50	13.4	10.1	353 7	6.0	77.0	127.8	225.9
50.00	10.1	7.6	471.6	4.5	103.1	170.5	301.1
75.00	6.7	5.0	707.4	3.0	155.1	255.7	451.7
100.00	5.0	3.8	943.2	2.3	207.0	340.9	602.3

six monitors will be required. Work surface space will be needed for the operator/video processor interface (typically a keyboard). The console will also provide the operator interface for controlling surveillance cameras (pan/tilt/zoom controls), when required.

(2) *Rack space.* The CCTV will require electronic rack space in proximity to the Security Center console. This space will house the video processor components, including master video sync, switcher, transmission system drivers and receivers, and video recorders. A CCTV system of average size will require approximately two 72-inch racks of standard width (19-inch). An efficient design will co-locate the alarm processor equipment in these racks or adjacent to them, to minimize lengths of required cabling between these tightly coupled systems.

(3) *HVAC.* The Security Center-based CCTV equipment will be of solid state construction and will present a moderate heat load to the HVAC system. For an average system, the heat load will be between 120 and 180 watts per linear foot of installed rack equipment. The designer will perform calculations to determine exact cooling requirements.

c. IDS alarm processor. The alarm processor is the most important interface for an effective CCTV assessment system. The layout and location of the IDS sensors dictate the number and locations of cameras and, therefore, the complexity of the CCTV system design.

(1) *Alarm-correlated video.* When the alarm processor receives an alarm, it must correlate the alarmed sensor location with a particular camera and send an appropriate selection command to the video switcher. In contemporary systems, this is accomplished by the use of software-based data structures (look-up tables).

(2) *CCTV-generated alarms.* A proper design allows the CCTV system to detect and report to the alarm processor attempts at tampering or degradation of system components (such as loss-of-video). The designer will ensure that the alarm processor annunciates these events and requires console operator acknowledgment.

d. Site power (commercial/emergency/uninterruptible). Commercial power is electrical power supplied by a utility company. Emergency power is supplied by a local on-site device, usually a diesel generator, when commercial power fails. However, when commercial power fails, there will be a delay of several seconds before emergency power is available. Uninterruptible power is a source that can provide power for a finite time in the absence of both commercial and emergency sources. A typical example of an uninterruptible power supply (UPS) is one where batteries supply electrical power via an inverter and are maintained fully charged while the commercial power source is available. The cost of UPS is high, compared with commercial or emergency power. Since outdoor lighting systems consume much more electrical energy than do sensors or cameras, they are typically provided with commercial and emergency power sources but not UPS. Typically, outdoor lighting fixtures will extinguish immediately upon loss of power. When emergency power becomes available, each lamp must restrike and warm up to reach full brilliance. This can take several minutes depending on lamp type. As a result, when commercial power fails, there will be an interval when the cameras will be "blind." The power source requirement for the CCTV cameras should normally be made no more stringent than that of the lighting system. Provisions must be made to back up the video processing computer so that it does not require a "reboot" after a short power outage.

CHAPTER 9

DATA TRANSMISSION

9–1. General

A critical element in an integrated electronic security systems is the data transmission media (DTM) that transmits information from sensors, entry control devices, and video components to display and assessment equipment. A DTM link is a path for transmission of data between two or more components, such as sensor and alarm reporting system, card reader and controller, CCTV camera and monitor, or transmitter and receiver. DTM links connect remote electronic security system components to the Security Center. An effective DTM link ensures rapid and reliable transmission of data, is resistant to compromise, and is conducive to rapid fault detection and repair. Its design encompasses selection of the transmission media, transmission technique, associated transmission hardware, and degree of security to be provided for the communication system.

9–2. Data Transmission Media

A number of different media are used in transmitting data between elements of an IDS, EECS, and CCTV system. These include wire lines, coaxial cable, fiber optic cable, and RF transmission.

a. Wire line. Wire lines are twisted pairs that consist of two insulated conductors twisted together to minimize interference by unwanted signals.

(1) Twisted pairs carry information over a wide range of speeds depending on line characteristics. To maintain a particular data communication rate, the line bandwidth, time delay, or the signal to noise ratio may require adjustment by conditioning the line. Twisted pairs are permanently hardwired lines between equipment sending and receiving data.

(2) The nominal bandwidth of unconditioned twisted pairs is between 300 and 3,000 Hz. Data transmission in twisted pairs, in most cases, is limited to 1,200 baud or less. Hardwired twisted pairs must be conditioned by the supplier in order to obtain operating speeds up to 9,600 baud.

b. Coaxial cable. Coaxial cable consists of a center conductor surrounded by a shield. The center conductor is separated from the shield by a dielectric. The shield protects against electromagnetic interference. Coaxial cables can operate at data transmission rates in the megabits per second range. Attenuation becomes greater as the data transmission rate increases. The transmission rates are limited by the data transmission equipment and not by the cable. Regenerative repeaters are required at specific intervals depending on the data rate, nominally every 2,000 feet to maintain the signal at usable levels. Coaxial cable supports data rates in excess of 9,600 baud. Because of its wide bandwidth, coaxial cable can carry large numbers of simultaneous voice conversations, high-speed data, and large numbers of television channels. Coaxial cable also provides excellent isolation from external noise and crosstalk. However, it is susceptible to surge and lightning-related disturbances.

c. Fiber optics. Fiber optics uses the wide bandwidth properties of light traveling through transparent fibers. Fiber optics is a reliable communications medium best suited for point-to-point high speed data transmission. Fiber optics is immune to radio frequency electromagnetic interference and does not produce electromagnetic radiation emission; hence, fiber optics can be used in secure areas. Fiber-optic DTM (not equipment) can be installed in explosive and flammable environments. Fiber-optic cables can tolerate most severe weather conditions and can be immersed in many fluids. The bandwidth of the medium is virtually unlimited, and extremely high data transmission rates can be obtained. The signal attenuation of high quality fiber-optic cable is far lower than the best coaxial cables. Where repeaters are required nominally every 2,000 feet for coaxial cable, they may be 1 to 2 miles apart in fiber-optic systems. The preferred DTM for electronic security system is fiber-optic cables unless there are justifiable economic or technical reasons for using other types of media. The justification will include a technical analysis and cost comparison of the use of fiber optics compared with other media.

d. RF transmission. Modulated RF can be used as a DTM with the installation of radio receivers and transmitters. An RF transmission system does not require a direct physical link between the points of communication and is useful for communicating over barriers, such as bodies of water and heavily forested terrain. A disadvantage is that signal power received depends on many factors, including transmission power, antenna pattern, path length, physical obstructions, and climatic conditions. Also, RF transmission is susceptible to jamming, and an adversary with an appropriately tuned receiver has access to it. The use of RF will be coordinated with the communications officer to avoid interference with other existing or planned facility RF systems.

9–3. Data Transmission Techniques

There are two basic types of communication links: point-to-point and muliplex.

a. Point-to-point links. A point-to-point link is characterized by a separate path for each pair of components. This approach is cost effective for several component pairs or when a number of scattered remote areas must communicate with a single central location.

b. Multiplex links. The multiplex link, also commonly referred to as a "multidrop" or "multipoint" link, is a path shared by a number of components. Depending on the number and location of components, this type of configuration can reduce the amount of cabling required. However, the cost reduction from reduced cabling is somewhat offset by costs of equipment required to multiplex and demultiplex data.

9–4. Data Transmission Hardware

a. Modem. The word *modem* is a contraction of modulator-demodulator, which describes its function. The digital output of a piece of equipment can be modulated by a modem to form an analog signal for use with DTM links that have been designed for analog transmission, such as wire lines. Conversely, a modem can also demodulate an analog signal to change it back to a digital signal. One of the popular forms of modulation is frequency shift keying (FSK). With this technique, the carrier frequency, say 1,700 Hz, is modulated plus or minus 500 Hz to represent a binary 1 or 0. Thus, a frequency of 2,200 Hz represents a 1 and a frequency of 1,200 Hz represents a 0. This technique is used for devices operating at speeds up to 1,800 bits/second. Other techniques, such as phase shift keying (PSK), are used to operate at higher speeds of 2,400 to 9,600 bits/second.

b. Line driver. Digital transmission over long distances produces pulse rounding, a condition in which the edges of a square-wave pulse are distorted from loss of high-frequency components and signal attenuation, which can result in lost data. A line driver is a device that supplies output power sufficient to transmit digital signals over extended distances. These devices are usually used for distances greater than 100 feet. They can operate at speeds up to 19.2 kilobits per second, although special units are available that operate at speeds greater than two megabits per second. There is a direct trade-off between higher speed and longer distance in line-driver applications.

c. Repeater. This device is used on long DTM links to regenerate signals to their original level and quality. Repeaters are available for all types of media, including wire line, coaxial cable, fiber-optic cable, and RF. The number required, their locations, and specific characteristics depend on the type of link used and required transmission rate.

d. Fiber-optic transmitters and receivers. Fiber-optic transmitters convert electrical signals into light signals appropriate for transmission through an optical fiber. At the receiving end of the communication link, fiber-optic receivers convert the light signals back into electrical signals. Fiber-optic transmitters and receivers must be selected to match electrical characteristics of the equipment and the size and type of optical cable used.

e. RF terminals. When an RF link is used, the RF transmitter modulates a carrier frequency with data to be transmitted. At the receiving end of the link, the RF receiver demodulates the carrier and reproduces the original data. The electrical characteristics of the RF transmitter and receiver must be matched with those of the equipment to be interfaced.

9–5. Data Transmission Security

Data links used to communicate status of IDS sensors or other sensitive information to the Security Center must be protected from possible compromise. Attempts to defeat the security system may range from simple efforts to cut or short the transmission line to more sophisticated undertakings, such as tapping and substituting bogus signals. Data links can be made more secure by physical protection, tamper protection, line supervision, and encryption.

a. Physical protection. All DTM within a building will be routed in rigid galvanized steel conduit. Conduit provides physical protection and protection from EMI/RFI. Exterior cables can be protected by direct burial. As a minimum, cables will be buried at least 30 inches below the surface or below the frost line, whichever is deeper. Whenever direct burial is planned, additional lines should be included in the cable to accommodate future expansion or for in-place spares. Physical protection can be enhanced by encasing the cables in concrete; however, this is expensive and should be specified only when necessary. It should be noted that physical protection only delays an adversary attempting to compromise a DTM link; it does not alert security personnel of the attempt. To be effective, the area around the DTM link should be patrolled periodically so that tampering can be detected before it is completed.

b. Tampering protection. All communication equipment, such as signal transmitters and receivers, will be installed in enclosures that protect the equipment from normal abuse and provide protection against forced penetration. The enclosures will be locked, and all hinged or removable covers will be equipped with tamper switches to detect unauthorized access. In addition, all other types of enclosures, housing, and fittings with hinged or removable covers will be equipped with tamper switches. Covers of pull and junction boxes provided to facilitate installation need not be provided with tamper switches if they contain no splices or connections; however, the covers will be welded or brazed in place.

c. Line supervision. Communication links can be compromised by learning the characteristics of the "no-alarm" signal, reconstructing the signal, gaining access to the link, and substituting bogus signals. To protect a DTM link, one or more of these steps must be prevented. This can be accomplished by using line supervision, which is, transmitting a continuous or coded signal through the data lines and monitoring the signal for changes characteristic of line faults or tampering.

(1) *DC supervision.* This technique is commonly used with wire lines, particularly those connecting an IDS sensor to an annunciator or local processor.

(*a*) A nominal value of direct current of typically around one milliampere is maintained in the link at all times. An alarm is generated whenever the current varies by more than a predefined amount above or below the nominal values. For example, a system with 10 percent supervision will generate an alarm when the current in the system varies more than 10 percent from its nominal value. Current supervision with sensitivities ranging from 5 to 30 percent is available.

(*b*) In IDS sensor applications, one or more resistors are wired in series or parallel with the tamper and sensor contacts. Typical circuit configurations are shown in figure 9-1. The top circuit illustrates use of a normally closed (NC) tamper switch with a normally open (NO) sensor contact. A DC voltage is applied to the line at all times and the resulting current, determined by source impedance and end-of-line (EOL) resistor, is measured. If the tamper switch is opened, the open circuit (no current) condition results in initiation of an alarm. If the sensor contact is closed, the EOL resistor is shorted, resulting in a current increase, which also initiates an alarm. To reduce the possibility of an adversary tampering with the circuitry, the EOL resistor should always be located near the sensor alarm contact.

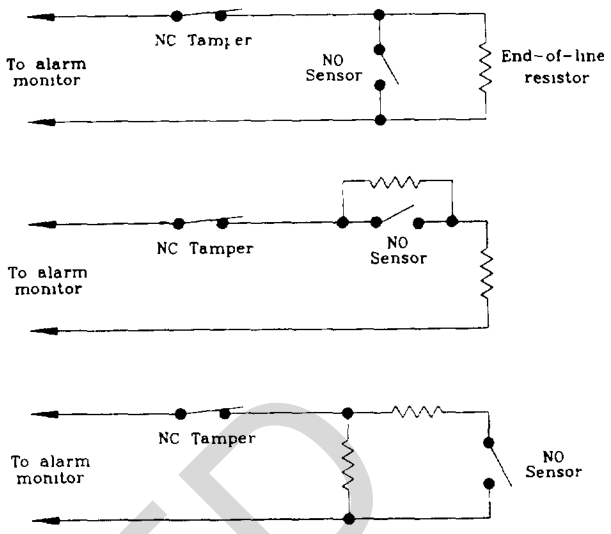


Figure 9-1. Examples of DC Supervision.

(2) *AC supervision.* This type of supervision uses alternating current, rather than direct current. The resistors at the end of the line are replaced by impedances, such as a coil or capacitor. Alarm criteria can depend on a change in both magnitude and phase of the signal.

(3) *Digital.* More and more security-related DTM links use digital transmission techniques. For example, multiplex systems use local processors to monitor status of multiple IDS sensors continuously. These processors convert sensor status information to digital data, which are transmitted to the Security Center. To make it difficult or impossible to record the no-alarm signal for playback later, some systems constantly change the no-alarm condition. For example, this can be accomplished by starting each scan cycle with a different address.

d Encryption. Security can be enhanced by encoding or encrypting digital data, that is, scrambling the data so it cannot be read without knowing the key or code. A commonly used algorithm is the Data Encryption Standard (DES), which has been adopted by the National Bureau of Standards for use by the Government. This algorithm uses a 56-bit key chosen by the user. Additional information on DES can be found in FIPS PUB 46-1. It should be noted that, regardless of the coding technique, this mode of operation has inherent weaknesses, because it is possible for an adversary to record the data and play it back later. To eliminate this possibility, a different key can be used to encode each bit, data word, or group of data words transmitted over the link. This requires that the receiving end of the link uses the same key in synchronism with the transmitting end.

9-6. Additional Considerations

a Environment. Communication lines and equipment are specified to operate under ambient environmental conditions expected at a specific site. Equipment and cable to be used indoors will be rated for continuous operation under ambient conditions of 32 to 122 degrees Fahrenheit and 10 to 95 percent relative humidity, noncondensing. As a minimum, equipment and cable to be used outdoors will be rated for continuous operation under ambient conditions of zero to 138 degrees Fahrenheit and 20 to 95 percent relative humidity, condensing. In some areas, more stringent requirement will be applied.

b. Transient protection. DTM equipment can be quite vulnerable to transients generated by nature (lightning), as well as by man-made systems. Transients induced into the system through communication lines and power lines can affect operation of the equipment. Transients caused by voltage surges or indirect lightning strikes can also physically damage equipment. The best method of protection is to eliminate sources of the transients; however, this is usually not possible. The next best method is to insert protective devices between sources and the equipment. Protective devices may be installed in series or in parallel. Series overvoltage protection requires that the protective device be able to swing from full conduction (with a very small voltage drop) to a virtual open circuit in a very short time. Hence, the device requires a high overvoltage rating. The equipment is also susceptible to damage if the device fails. For this reason, parallel (shunt) protective devices are generally used. A variety of transient protection devices is available, including gas tubes, air gaps, varistors, zener diodes, and optical isolators. Additional information on surge protection devices can be found in ANSI C62.31, C62.32, and C62.33. All cables, other than fiber optic, that serve as communication links should have transient protection devices installed at each end.

c. Power supply requirements. As with other electronic security system equipment, all communication equipment should be operable from commercial electric power. Provisions should be made for automatic switchover to backup power without loss of data, in the event of commercial power failure. Backup power may be supplied by batteries or an UPS. Data communication equipment should be provided with the same backup capacity as the equipment it serves.

d. Economic considerations. The cost of a DTM link depends primarily on the type of medium used, length of the link, and type of environment (interior or exterior) through which the link is routed.

(1) Cable designed for exterior applications, such as direct burial cables, are more costly than those designed for interior applications. When underground rodents are a problem, direct burial cables with an outer protective armor sheath will be used.

(2) Additional equipment, such as modems, line drivers, and fiber optic transmitters/receivers will also be required.

CHAPTER 10

INTERFACES

10-1. General

In preparing an electronic security system design, the designer must keep in mind the fact that IDS is not a stand-alone entity. Interfaces with several external systems and services must be carefully planned and incorporated into the design.

10-2. Electrical

Electrical power provides energy necessary to maintain operation of the electronic security system. One hundred percent availability of IDS is usually required, and depending on site requirements some components of the CCTV and EECS may require 100 percent availability; any exception must be clearly documented and approved prior to design by the responsible command. A site's electrical power is of three types: commercial, emergency, and uninterruptible. The three are complementary and must be used together to provide power continuously without interruption. A basic block diagram is shown in figure 10-1. Additional information on power system requirements can be found in TM 5-811-2.

a. Commercial power. This power is supplied from the site power grid. Generally, a single-phase, three-wire, 120/240-volt or three-phase, four-wire, 208Y/120-volt, 60-Hertz system will be used, depending on requirements of specific electronic security system equipment. This power interface will be distributed from new or existing circuit breaker panels. The designer will be required to locate new transformers, grounding, power panels, and cable runs where necessary. The operating history of commercial power services will be reviewed to ascertain the frequency and duration of outages. The data provide information necessary in determining capacity of the emergency power source.

b. Emergency power. An alternate power source is required when normal power is interrupted for finite periods of time, usually greater than 3 minutes. This source should have sufficient capacity to operate the entire electronic security system load, including lighting. Emergency power is usually supplied from engine-generator sets. These units may already exist, with sufficient spare capacity to add the electronic security system load. If not, the designer will include the necessary emergency power provisions in the design. Emergency power must be capable of continuous operation, with on-line refueling. It must be capable of switching from- commercial power to emergency power and back again.

c. Uninterruptible power. Some types of electronic security system equipment, such as processors with solid-state memory, cannot tolerate short interruptions of power, which will occur during switchover from the commercial power to an engine-driven emergency power source. This volatile electronic security system equipment must be powered from an UPS or battery source.

(1) A UPS consists of a rectifier, batteries, and inverter. If incoming power is interrupted, the UPS automatically supplies an uninterruptible source of ac power. UPSs are generally used where large concentrations of equipment are located, such as at the Security Center. The battery should be sized for approximately 30 minutes of operating capacity. However, if the site does not have an emergency power source, the UPS battery should have a minimum of four hours operating capacity.

(2) Many types of electronic security system equipment, particularly equipment for remote locations, are furnished with an integral battery backup supply. The designer will specify a battery that will provide a minimum of 4 hours of backup power under rated temperature conditions. Exact site requirements must be determined and emergency power provided accordingly.

d. Grounding. The designer will review grounding practices for all electronic security system equipment and the equipment on which it is mounted to ascertain that a complete stable instrumentation quality grounding system design is accomplished.

10-3. Civil

Civil engineers must investigate and plan for changes to accommodate deployment of exterior electronic security system components. Deployment will be affected by existing physical features such as fencing and gates, terrain, trenching, poles, relocation of existing services, roads, and culverts.

a. Fencing and gates. Fencing must be in good repair. Fences and gates are often used as a medium on which intrusion detection sensors are located. Consequently, they must be properly tensioned and grounded. Fences must be straight to facilitate sensor installation and not obstruct the field of view of cameras.

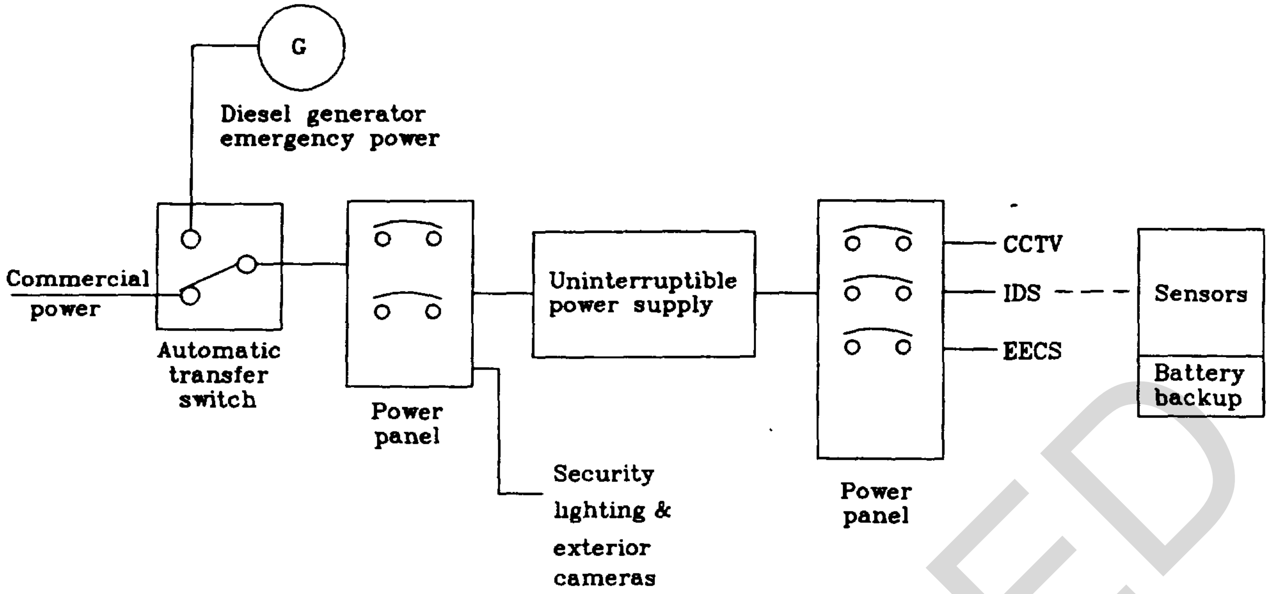

G
Diesel generator emergency power
Commercial power
Automatic transfer switch
Power panel
Uninterruptible power supply
Security lighting & exterior cameras
Power panel
CCTV
IDS
EECS
Sensors
Battery backup

Figure 10–1 Electronic Security System Electrical Power Block Diagram

b. Terrain. Terrain between fences and on either side is required to be graded and grubbed. Grading ensures that line-of-sight for sensors and assessment cameras is such that there will be no areas lacking coverage. Grubbing ensures that vegetation does not cause nuisance alarms and does not provide concealment for adversaries.

c. Trenching. Data communication and electrical power cables are usually routed from the Security Center to remote locations of interior and exterior electronic security system equipment through trenches, although some use of aerial installations is permitted. Trenching considerations include route, depth, width, and quantities.

d. Poles. Poles are used to support a variety of electronic security system components, such as lighting, sensors, cameras, line-of-sight RF transmitters/receivers, and cable transmission systems. Each pole must be properly located with respect to fencing and IDS zone boundaries. They must be of sufficient strength and height for equipment they will support.

e. Existing services, roads, and culverts. The last significant civil concern is relocation of interfering existing services, such as buried or overhead cabling, relocation of roads, and installation or modification of culverts. Culverts are needed to prevent rain or melted snow from running across IDS sensor zones and creating nuisance alarms, degrading sensor performance, or creating terrain washout. Since culverts can be used for concealed movement by adversaries, they must be protected accordingly.

10–4. Mechanical

The primary mechanical engineering function is to ensure that electronic equipment in the Security Center is adequately ventilated and cooled. The Security Center has additional constraints because of the presence of guards, whose comfort must be considered. Another consideration is hardening the Security Center against chemical agent attack. The potential for chemical agent attack will be part of the site-specific threat statement.

10–5. Structural

The structural engineering function is required to ensure equipment is protected against intruder actions. Protection takes the form of uniform hardening of walls, floors, ceilings, doors, glazing, and utility penetrations against the adversary use of hand tools, power tools, thermal tools, explosives, and weaponry. An important consideration in hardening is to accomplish it in a cost effective manner. It is also essential to review and ensure uniformity of hardening for vital equipment that may be located in different rooms. If the operator console and electronic equipment are in one room, and the backup electrical power source in another, a single point failure of either will cause loss of the security system; therefore, the two rooms must be uniformly hardened.

10–6. Architecture

The architectural function is to ensure that the security center and critical rooms within the center are integrated and located for maximum protection. Key rooms, such as the security center, should not be located on exterior building faces susceptible to stand-off weapon attacks from outside the protected area. Where possible, all critical rooms should be located near the center of the building, away from exterior walls and roof. Interior location limits use of explosives and will hinder an adversary's gaining access to protected assets. In multipurpose buildings, critical security areas should be located away from the general building population, including visitors. The use of glazing and doors will be minimized. When multiple doors are used, the doors will be interlocked in such a way that uninterrupted passage can not be achieved.

10-7. Other Interfaces

The electronic security system also has critical interfaces with other elements, such as contraband detectors, security lighting, voice communications, barriers, security personnel, policy and procedures, testing and maintenance. TM 5-853-1 details the procedures for interfacing electronic security systems with barriers and other physical security components.

10-8. Health/Safety and Fire

Both the health/safety and fire functions must be considered in design of an electronic security system. If electronic security system components are to be used in hazardous locations, only equipment and associated wiring approved as intrinsically safe for these locations will be used. Health/safety may require emergency egress from security areas, while fire and emergency personnel may require emergency ingress. Clearly, movement of personnel to and from the security area is of utmost importance in emergencies, but control of the area for security purposes is also required so that the area is never compromised. The designer must achieve a working balance of these sometimes competing interests.

10-9. Operations

Electronic security systems are used by DA to ensure that mission-essential vulnerable areas can perform their function in the defense of the United States. Security must protect assets yet permit their primary operation to continue effectively and efficiently. The electronic security system must co-exist and support operational personnel as they enter and leave a facility, work within a facility, and when they secure their facility. Each of these operational modes must be considered in design of the electronic security system. Vulnerabilities will be minimized at all times. An electronic security system is most vulnerable during normal operations because many interior sensors are in the access mode, secure containers are open, doors are being opened and closed, CCTV is generally restricted to surveillance, and inside intruders can act covertly or overtly. The most secure profile is off-shift because those conditions no longer exist. The electronic security system designer will review the entire operational profile of a facility and its personnel, to ensure balanced protection through the use of carefully selected hardware, software, and installation requirements.

CHAPTER 11

PROJECT IMPLEMENTATION

Section I. DESIGN CONSIDERATIONS

11-1. General

a. This chapter describes development of the top-down design process. Depending on the level of protection required, new facilities may require both interior and exterior electronic security system elements. The applicable regulations, threat, and design criteria will define the general requirements of the electronic security system. For existing electronic security systems, hardware and software may need to be supplemented, upgraded, or completely replaced.

b. A site layout is required, in which all assets are identified and located. The site layout will also be a useful design tool for such tasks as configuring the DTM media described in chapter 9.

c. The exterior and interior intrusion detection systems should be configured as layers of unbroken rings, concentrically surrounding the asset. These rings should correspond to "defensive layers" constituting the delay system. The first detection layer is located at the outermost defensive layer necessary to provide required delay. Detection layers can be on a defensive layer, between layers, or on the asset itself, depending on delay required. For example, if a wall of an interior room provides sufficient delay for effective response to the aggression, detection layers could be between the facility exterior and interior room wall or on the interior room wall. These would both detect the intruder before penetration of the interior wall is possible.

11-2. Basic Guidance

a. IDS is deployed in and around the delay system (barriers) as detailed in TM 5-853-1. Voice communication links (radio, intercom, and telephone) with the response force are located in the security center. The center is manned by security personnel who will use communications to alert and dispatch response forces in event of an alarm.

b. To ensure that barrier integrity is maintained against intruders, the barrier should always be deployed behind the IDS. An intruder will then activate the alarm sensor before penetrating or bypassing the barrier(s), thus providing delay for alarm assessment and response. The delay time, in fact, is the determining factor in whether assessment is conducted by dispatching a guard or by CCTV observation. Normally, an intruder can climb a fence before a guard can be dispatched; hence, CCTV assessment is usually required with exterior IDS. Barriers can be located ahead of an alarm sensor as boundary demarcation and can serve to keep people and animals from causing nuisance alarms by inadvertently straying into a controlled area. However, such barriers provide no additional response time because the barrier would be breached before the IDS sensors would have been activated.

c. Data for monitoring and controlling the electronic security system are gathered and processed in the Security Center. There the operator interacts with information from the electronic security system components located at remote facilities.

d. The preferred medium for transmitting data in an IDS project is a fiber optics system dedicated to the project. It provides for communications not susceptible to voltage transients, lighting, electromagnetic interference, and noise. Additionally, the fiber optics DTM provides communication line security and wide bandwidth for video signals and increased data transmission rate. The DTM for IDS projects will be fiber optics unless there are justifiable economic or technical reasons for providing other DTM types.

11-3. Electronic Security System Effectiveness

a. An IDS has a degree of protection effectiveness that is based on its probability of detecting intruders attempting to go over, under, around, or through the physical security system, using forced entry, covert entry, or insider compromise. A well-designed system will minimize the possibility of successful use of covert entry or insider compromise. Interior and exterior alarm sensors have a figure of merit, called the probability of detection, based on capability to detect an intruder passing through a sensing field. An intruder disturbs the steady-state quiescent condition of a sensor for a finite period of time. Sensors are designed to detect a person of minimum stature, moving within a specific range of speeds and distance from the sensor, and any target outside of those parameters will probably not be detected. The probability of detection (PD) for a specific sensor is usually specified at 0.9 or greater, but the designer must be aware that the probability of detection is based on certain target constraints and environmental conditions. Most manufacturer's literature does not specifically mention that performance of sensors will be degraded as a result of environmental conditions and covert intruder techniques.

b. Another topic not usually discussed in manufacturer specifications is environmental or nuisance alarms, which can be caused by climatic conditions, such as wind or rain, or by intrusion of animals or birds. The alarm annunciation is valid because the sensor's thresholds have been exceeded; however, the alarm does not represent a valid penetration attempt. If the assessment system is slow, the operator may not be able to determine the cause of the alarm and must, therefore, treat an environmental or nuisance alarm as real.

c. A third type of alarm is a false alarm that is caused by electronic circuit tolerances being exceeded, which results in actuation of the sensor. False alarms may also result from improper installation of the sensor or from effects of other equipment in the immediate area, such as an ungrounded fence.

d. After an alarm is sensed and information is displayed in the Security Center, the operator must determine the cause of the alarm (i.e., intrusion, nuisance, environmental, false). Timely assessment is required to determine its cause. For example, if an intruder scales a fence in 10 seconds and runs 20 feet per second, the intruder will have overcome the barrier and be 2,200 feet from the point of penetration in 2 minutes. To conduct an accurate assessment of the alarm, after 2 minutes, guards will have to search an area of approximately 200 acres. A fixed television camera properly located and integrated with the alarm processor can accomplish assessment while the intruder is still in the controlled area. Figure 11-1 is a graphic comparison of the relative difficulty of video and guard assessment.

e. A high-level security IDS must have a fixed television camera for each alarm zone, although some zones may be viewed by more than one camera because of topography. For a CCTV camera to be effective, the area it views must be adequately lighted. To correlate the alarms and cameras in a large system (more than 10 cameras) in a timely manner, a computer-based processing system must be used to select and display alarms and camera scenes for the operator. A complex electronic security system, therefore, has the following basic components:

(1) Alarm sensors.
(2) Assessment (CCTV or personnel).
(3) Computer based processing system.
(4) Operator displays.
(5) Security lighting.

f. The IDS is normally deployed in a series of concentric layers. Overall probability of detection improves with each added layer of IDS. The layers (interior and exterior) should be functionally uni-

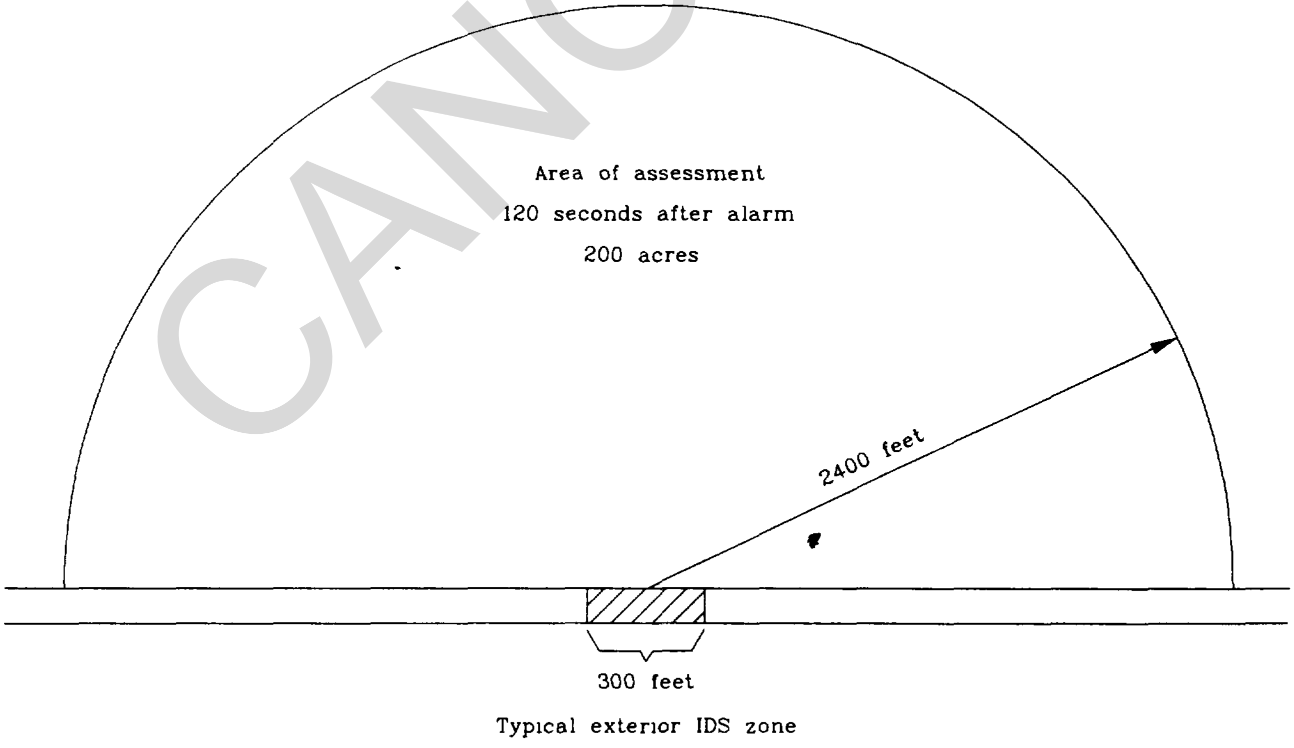


Figure 11-1. Comparative Areas of Assessment by CCTV or Guard.

form; however, their overall effectiveness and cost are different.

(1) The exterior zones are significantly different from the interior zones because of the following considerations:

(*a*) Probability of detection.

(*b*) Cost per detection zone.

(*c*) Number of zones.

(*d*) Overall sensor coverage.

(2) A single interior sensor has a probability of detection several orders of magnitude greater than an equivalent exterior sensor because it is not subject to such wide variances in environmental conditions. This is true because detection probability is not measured at all times but only during an attempted penetration by an intruder. Typically, sophisticated intruders will attempt their penetration and challenge an IDS under conditions most favorable to themselves. During inclement weather (fog, snow, rain) the exterior components (sensors, CCTV, lighting) are less likely to detect a penetration attempt, and since the interior IDS is less influenced by environmental conditions, it is more likely to detect the penetration attempt.

(3) Another consideration in comparisons of interior and exterior IDS is cost. Because of environmental conditions, the exterior electronics must be designed and packaged for extremes of temperature, moisture, and wind. The result is that exterior electronic packages are more costly than equivalent packages for interior applications.

(4) A third consideration is the number and size of detection zones required for exterior IDS as compared with those of interior IDS. Lineal distances and number of zones for an exterior IDS may be as much as ten times those of an interior IDS.

(5) The fourth consideration is that a state-of-the-art exterior IDS does not detect penetration attempts above the height of the fence (typically 8 feet). Fence-mounted sensors are usually limited to this height because the fence fabric or poles are used to support the sensor. For above-ground sensors in the controlled area between the fences, the detection height is limited by the sensor mounting brackets and posts. In some applications of field sensors, especially buried sensors, the detection height is no more than 3 feet. For a facility, an interior IDS can be deployed on the walls, floor, or ceiling, thus permitting complete protection of the asset.

(6) Relationships of interior and exterior IDSs developed in preceding paragraphs indicate that an interior IDS may be orders of magnitude less costly than a comparable exterior IDS. This comparison indicates to the designer the value of selecting and deploying a well-planned, well-designed, layered IDS. The basic rule in overall design of an IDS is to design from the inside-out, that is, layered from the asset to the site boundary.

g. Results of comparative analysis of EECS for interior or exterior applications are not equivalent to those for IDS. Generally, interior and exterior applications are equivalent because the components are deployed in a building. The difference between the two applications is merely that an interior electronic entry control system generally screens a smaller population than does that at the exterior perimeter, and interior screening usually does not involve vehicles.

h. In summary, the electronic security system designer must decide where to locate the IDS, how many layers to use, and relative effectiveness of each layer. Regardless of relative merit of an interior or exterior IDS, it is prudent to deploy both; often, in fact, regulations require both systems. It is important that the designer appreciate relative merits of each and understands how to deploy them for maximum synergistic effects.

11–4. Interior IDS Considerations

a. An interior IDS is typically deployed within a building boundary in the immediate vicinity of the asset being protected. This system has the advantage that probability of detection is not affected by outside environment. Also, effectiveness of the physical security system is enhanced by the fact that interior barriers (walls, ceiling, floor) inherently impose longer delay than exterior barriers (fences and gates).

b. Functionally, an asset should be viewed as being contained within a cube, with IDS protecting all six faces. An IDS can be deployed at the cube's perimeter, in its interior space, or in the space immediately outside the cube. The importance of delay, represented by the cube's surface, would indicate that preferred IDS deployment is outside space followed by perimeter followed by inside space.

c. A simple example of interior IDS application is protection of an igloo. In this example, the igloo is on grade and all of its exposed surfaces are bermed, with exception of the headwall. An IDS on the exterior face of the igloo is subject to outside environmental effects. The igloo's exterior protection function may be accomplished by the site perimeter IDS. The door in the headwall should be equipped with sensors to detect opening, and penetration sensors should be deployed on the headwall and door surfaces if construction is weak. The interior of the igloo may al~~so~~ have a volumetric sensor. A CCTV camera may be located within the igloo to assess penetration of exposed headwall/ door surfaces and of interior space.

d. If the building is large enough, multiple layers of interior IDS may be deployed for a given asset if this increased level of protection is dictated by the threat assessment performed per TM 5-853-1. A multilayered interior IDS will improve the overall probability of detection.

11-5. Exterior IDS Considerations

a. An exterior IDS is typically deployed at the boundary of a site or some other significant boundary such as the demarcation fence for a group of igloos. The exterior IDS has the advantage that it remains in the "secure" mode at all times.

b. The ideal configuration for an exterior IDS is a rectangle or a polygon, all sides being straight. The IDS is located in and around barriers that are typically dual fences. The outside fence is used for demarcation, the interior fence to aid detection and provide some delay. If dual fences are not required by regulation, the sensors would be deployed on the fence or inside of it.

c. Previous chapters described sensors and assessment cameras available to the designer at present. Figure 11-2 shows a typical cross-section of an exterior IDS. For important assets, multiple and diverse alarms can be used to improve probability of detection. Note that on the plan view an exterior IDS the CCTV camera is located well outside the physical limits of a particular zone because of limited field of view of the camera.

11-6. Physical Considerations

As discussed in chapter 4 probability of detection for all IDS components is based on ideal conditions, but IDS capabilities are also affected by other elements, such as topography or geometry. A line-of-sight component cannot be effective in a bend, undulation, or corner in either the horizontal or vertical plane. In placement of IDS hardware, the designer must take care to avoid introducing vulnerabilities by not correcting mitigating physical features that reduce or eliminate detection capabilities.

Section II. DESIGN METHODOLOGY

11-7. Design Sequence

Design of an electronic security system will proceed through a relatively fixed sequence of events, such as shown in figure 11-3.

11-8. Preparation of Design Criteria

Through the risk analysis and threat assessment process detailed in TM 5-853-1, the installation/ MACOM will have prepared a list of security

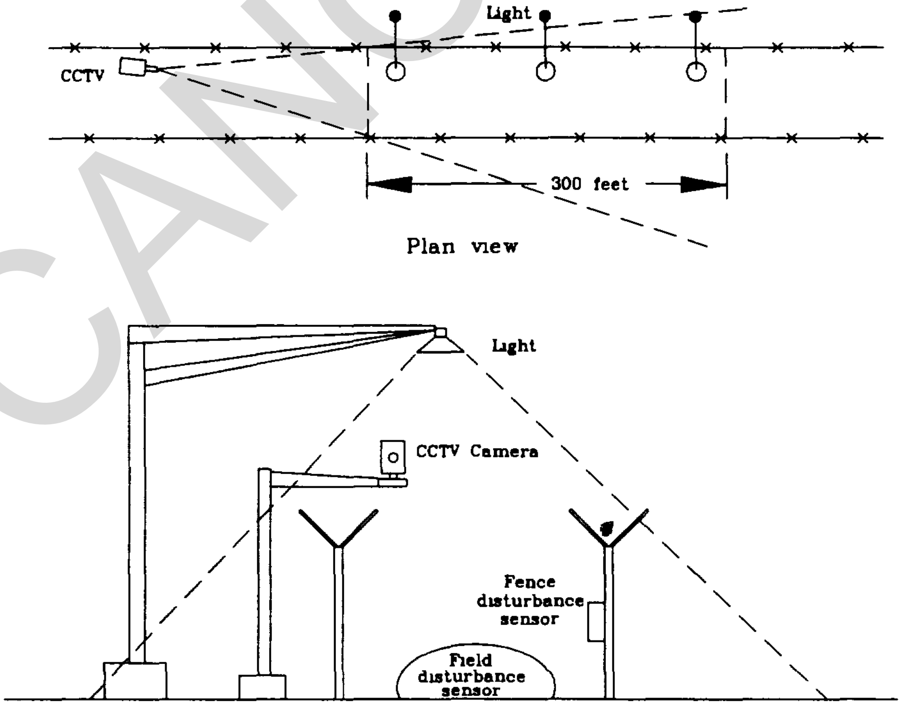


Figure 11-2. Exterior IDS Configuration.

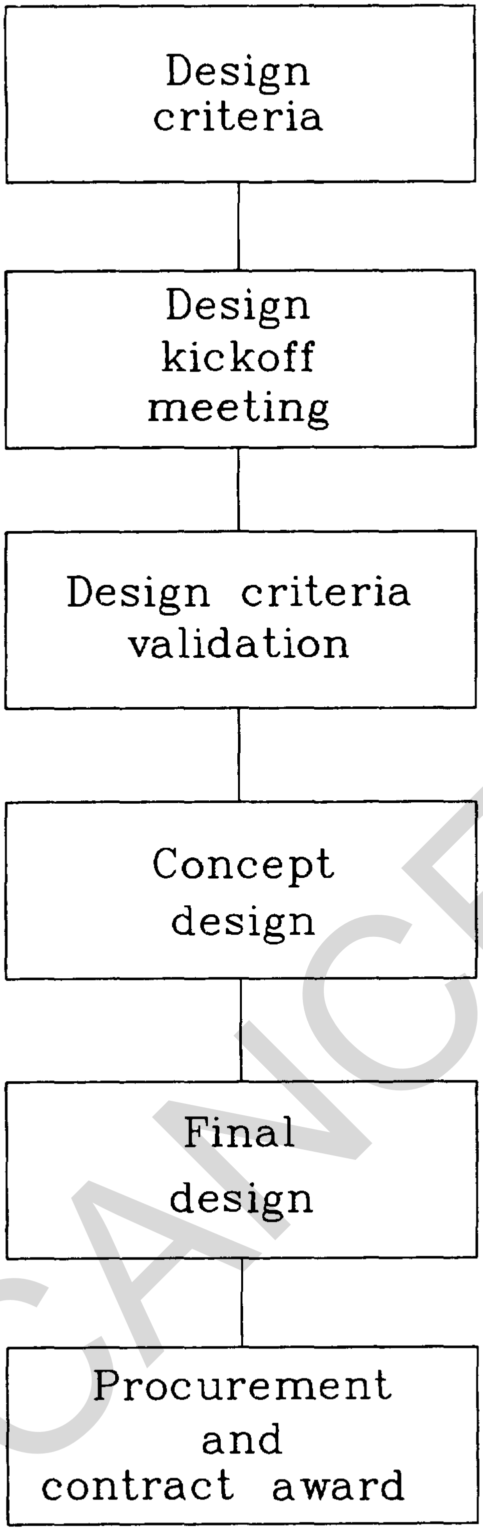


Figure 11-3. Sequence of Design Development Events.

areas to be included in the electronic security system. This initial work will determine which assets are classified as mission essential vulnerable areas (MEVA) or restricted .areas and the security level (A, B, C, D) associated with each asset. It will also have determined the location of the Security Center(s). These activities will have been performed in sufficient detail for preparation of design criteria and supporting documentation (by others). An example of such design criteria is that included on the DD Form 1391 and supporting documentation, which would be used in the case of an MCA-funded project. The design criteria provide the basis for the electronic security sytem design. The designer must determine whether or not standard military hardware is required to be used and if so, whether or not it satisfies the requirements. If commercial hardware is to be used, the designer will verify that a waiver for the use of commercial hardware exists.

11-9. Design Kickoff Meeting

a. One of the first activities the designer will set up is a design kickoff meeting. This meeting will cover scope of the project, anticipated problem areas, scheduling of survey and other work required at the site, and identification of all organizations to be contacted during the design process. The following personnel should be in attendance:

(1) Government design representative.

(2) Architect-engineer (AE) design representative (when appropriate).

(3) Director of Engineering and Housing representative.

(4) Provost Marshal office representative.

(5) Communications office representative.

(6) Other personnel as required.

b. A necessary task in design of electronic security systems is to retrieve pertinent information related to the areas that are to be included in the project. The information to be retrieved includes the following:

(1) As-built drawings of the security areas.

(2) Lists and schedules of any existing electronic security system equipment.

(3) Lists and schedules of security areas requiring special consideration.

(4) Applicable Army regulations and standards.

(5) Applicable special requirements at the site.

11-10. Design Criteria Validation

The next step in the design process is to validate design criteria. The design criteria basis is usually a security engineering survey report that was generated earlier. The design team will visit the site and validate survey report data and findings. All recommendations will be reviewed and validated, or appropriate changes due to any changed conditions or new requirements will be noted. All documented information, such as drawings and lists of existing equipment, will be verified by comparison with actual conditions in the field. A validation report will be prepared, summarizing finding of the survey validation and pointing out any discrepancies, problem areas, and changed requirements.

11-11. Concept Design

The concept design phase represents approximately 35 percent of total project design effort. It will provide a complete description of the electronic security system project. The concept design documentation package will include drawings, design analysis, outline specifications, and a preliminary construction cost estimate.

a. Drawings. The drawing package will include—

(1) Title sheet (100 percent complete).

(2) List of abbreviations and symbols (100 percent complete).

(3) Site plan (100 percent complete).

(4) IDS block diagram, including data transmission (100 percent complete).

(5) IDS zones and sensor installation design (35 percent of total).

(6) All details associated with installation of items in (5) above (35 percent complete).

(7) CCTV assessment block diagram, if applicable (100 percent complete).

(8) Entry control system block diagram, if applicable (100 percent complete).

(9) Security Center equipment layout and arrangement (100 percent complete).

(10) Security Center power, lighting, heating, ventilation, and air conditioning details (35 percent complete).

b. Design analysis. The design analysis will include a narrative discussion of design philosophy and assumptions, reference sources, and design calculations. It will also outline alternative systems, arrangements, and hardware that were considered, and the rationale for selecting the recommended concept design over the alternatives.

c. Outline specifications. These will briefly describe the type and quality of required construction, construction materials, and equipment.

d. Preliminary construction cost estimate. As a minimum, this will include cost estimates of the following:

(1) Electronic security system components and materials.

(2) Installation of electronic security system components and materials.

(3) Required modifications to and repair of existing electronic security system components.

(4) Security Center hardware, software, and data base installation.

(5) Data transmission components, material, and installation.

(6) Construction and site work to support electronic security system installation.

(7) Training.

(8) Operation and maintenance manuals.

(9) Maintenance and service for the first year (including spare parts).

11-12. Final Design

The final design phase is divided into three stages, which are intermediate design, final design, and final submittal.

a. Intermediate design. This stage carries the project design effort to about 60 percent completion. Drawings and design analysis will be updated to incorporate all changes and revisions based on approved comments from review of the concept design. In addition, approximately two-thirds of the IDS installation design will be completed. Marked-up source specifications with annotations to justify any additions, deletions, and modifications will be provided. Draft specifications for all areas not included in source specifications will be prepared.

b. Final design. All drawings and documents will be 100-percent complete at the end of this stage. Documents will be updated to incorporate all changes and revisions, based on approved comments from review of the intermediate design. During this stage of design, the project site will be visited to verify all project drawings and specifications are complete and accurate. The preliminary construction cost estimate will be updated to reflect cost based on the final design. The final design package will be forwarded to appropriate construction division personnel for performing a constructability review. The following documents will be prepared and included with the final design package:

(1) Proposal evaluation guide.

(2) Technical requirements list.

(3) Technical requirements score sheet.

c. Final submittal. All final design documents will be updated to incorporate approved comments, including those from the constructability review, of the final design. The final cost estimate will be corrected as necessary. All original mylars and updated versions of the other final design documentation will be submitted.

11-13. Procurement and Contract Award

Functions to be performed by the designer during procurement will include preparation of special procurement clauses, proposal evaluation data including assignment of point scores to scoresheets, and participation in technical proposal evaluations. An AE is normally excluded from any participation in RFP evaluations. After contract award, the designer should be involved in numerous interdependent activities, including review meetings, submittals review, and testing. Timely completion of the project requires that the contractor have sufficient technical personnel to complete tasks within the designated schedule and that the Government's Quality Verification organization perform its functions in a correct and timely manner.

APPENDIX A

REFERENCES

Government Publications

Department of the Air Force

SAFE-SIT-0001	Siting Criteria for SAFE Programs

Department of Defense

DOD 3235.1	Test and Evaluation of System Reliability, Availability, Maintainability—A Primer
DOD 5200.1-R	Information Security Program Regulation
MIL-HDBK-759	Human Factors Engineering Design for Army Material
MIL-STD 1472	Human Engineering Design Criteria for Military Systems, Equipment, and Facilities

Department of the Army

AR 190-13	The Army Physical Security Program
AR 380-5	Army Information Security Program
TM 5-811-2	Electrical Design, Interior Electrical Systems
TM 5-853-1/ AFM 88-6, Volume 1,	Security Engineering Project Development
TM 5-853-2/ AFM 88-6, Volume 2,	Security Engineering Concept Design
TM 5-853-3/ AFM 88-6, Volume 3,	Security Engineering Final Design
TM 5-6350-264-14-1	Installation, Operation, and Checkout Procedures for Joint-Services Interior Intrusion Detection System (J-SIIDS)
TM 11-6350-219-13	Remotely Monitored Battlefield Sensor System (REMBASS) System Manual

National Institute of Standards and Technology (NIST)

National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161

FIPS PUB 46-1	Data Encryption Standard
FIPS PUB 94	Guidelines for Electrical Power for ADP Installations

Federal Communications Commision (FCC)

Superintendent of Documents, US Government Printing Office, Washington, DC 20402-9325

FCC Part 15	Rules and Regulations: Radio Frequency Devices

Nongovernment Publications

American National Standards Institute (ANSI), 1430 Broadway, New York, NY 10018

ANSI C62.31	Gas-Tube Surge-Protective Devices, Test Specifications for
ANSI C62.32	Low-Voltage Air Gap Surge-Protective Devices, Test Specifications for
ANSI C62.33	Varistor Surge-Protective Devices, Test Specifications for
ANSI X4.13	Financial Transaction Cards
ANSI X4.16	Magnetic Stripe Encoding

American Society for Testing and Materials (ASTM), 1916 Race Street, Philadelphia, PA 19103

ASTM F 967	Standard Practice for Security Engineering Symbols

Electronic Industries Association (EIA), 2001 Eye Street, NW, Washington, DC 20006

EIA–170	Electrical Performance Standards—Monochrome Television Studio Facilities
EIA–330	Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1
EIA RS–232–C	Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange
EIA RS–422–A	Electrical Characteristics of Balanced Voltage Digital Interface Circuits

Institute of Electrical and Electronics Engineers (IEEE), 445 Hoes Ln., Piscataway, NJ 08855–1331

IEEE Std 142	IEEE Recommended Practice for Grounding of Industrial and Commerical Power Systems

National Fire Protection Association (NFPA), 60 Batterymarch Street, Boston, MA 02110

NFPA 70	National Electrical Code

APPENDIX B

FACILITY SECURITY LEVEL AND IDS REQUIREMENTS

Table B-1. Facility Security and IDS Requirements

Type of Facility	*Typical Level of Security*	*Applicable IDS Requirements*
Ammunition and explosives storage rooms, facilities, or areas.	B	AR 190-11 DARCOM SUP-1
Arms storage, manufacturing, rebuild, and demilitarizing facilities and areas	B	AR 190-11
Army airfields and aircraft parking and maintenance areas.	B/C	AR 190-51
Banking institutions	C	AR 37-103
Billeting officer	D	AR 190-51
Book stores	D	
Bulk storage areas	D	AR 190-51
Chemical storage sites	A	AR 190-59
Classified sites or locations	A/B	AR 380-5 AR 380-19 DIAM 50-3
Cold storage facilities	D	AR 190-51
Command post (main and alternate)	B/C	
Commissaries	D	AR 190-51
Communications centers	B/C	AR 190-16
Communication facilities	B	AR 190-16
Consolidated supply/storage operations	D	AR 190-51
Controlled drug/narcotic vault/storage areas	C	AR 190-50
Data processing/computer terminal locations, facilities, and alternate facilities	B/C	AR 380-19
Demilitarization activities	C	
Field maintenance shops	D	AR 190-51
Finance offices	C	AR 37-103
Intrusion detection system monitor stations	A/B/C/D	
Medical supply storage facilities	C	AR 190-50
Motor pools	D	AR 190-51
Museums	B/D	AR 190-18
New construction projects	D	
Nuclear storage sites	A	AR 50-5
Open messes	D	
POL storage and dispensing points	C	AR 190-51
Pharmacies	C	AR 190-50
Post exchanges	C	AR 190-16 AR 190-51
Post offices	C	DOD 4525.6-M
Power supply transmission facilities (alternate and primary)	B/C	
Property disposal areas	C	
Quartermaster stores	C	AR 190-51
Research, Development, Test, and Evaluation Facilities	C	AR 70-65
Rod and Gun Clubs	B/D	
Sensitive compartmented information facilities (SCIFs)	A	DIAM 50-3
Shipping and receiving terminals	C	AR 190-51
Special service activities	D	
Supply and equipment pools	C	
Unit mail rooms	C	
Water sources	C	

APPENDIX C

SURVEY PROCEDURES FOR ELECTRONIC SECURITY SYSTEMS

C–1. Purpose and Scope

a. Site surveys. The purpose of site surveys is to identify electronic security systems equipment required to protect an installation against various threats, as defined by the MACOM/site. This is done by gathering on-site information, assessing the site, preparing design criteria,and preparing a cost estimate for design and construction. The site survey will provide an assessment of the existing security of the installation and a vulnerability analysis that will summarize modifications or additions required to satisfy the physical security requirements. Electronic security systems requirements will be determined by the site survey and will be documented in a report that recommends measures required to provide a new security system or to upgrade an existing system. The site survey report will include design criteria. The site survey will be scheduled to provide adequate lead time for programming, planning, design, and construction of the new or modified electronic security systems. The site survey will include—

(1) Descriptions of the site to be protected.

(2) Descriptions of the existing security system.

(3) Descriptions of vulnerabilities of the existing system.

(4) Recommend corrections of vulnerabilities.

(5) Detailed new protection dimensions and locations.

(6) Design and construction cost estimates of- proposed new protection. Items c, d, and f will be submitted under separate cover from the survey report, as they must be classified.

b. DOD policy for physical security equipment acquisition. DOD policy for physical security equipment acquisition is to acquire an effective, standard security system at a reasonable cost to ensure protection of DOD resources, commensurate with the degree of threat. If there is no DOD standardized system that can satisfy the requirement, commercial physical security equipment, acceptable to the MACOM, may be used.

C–2. Responsibilities

The following are principal participants in the site survey process:

a. Site survey process. The responsibilities of each of the participants are desribed below. This guide is limited to the site survey process. Planning and implementing the installation of physical security systems will be in accordance with AR 190–13.

(1) USACE IDS–MCX.

(2) MACOM.

(3) Installation Commander.

(4) Provost Marshal/Installation Security Officer.

(5) Director of Engineering and Housing. (DEH)

b. USACE IDS–MCX. The USACE, IDS–MCX is responsible to ensure the proper design, installation, testing, and checkout of DA electronic security systems projects. The IDS–MCX serves as point of contact between the site survey team and other agencies involved in the survey. The IDS–MCX has been chartered by AR 190–13 to—

(1) Conduct site surveys upon request.

(2) Provide technical assistance for electronic security systems projects.

(3) Develop electronic security systems guidance for design and construction.

(4) Coordinate technology transfer of electronic security systems within and between the Services.

(5) Ensure electronic security systems design consistency and compliance with DA standards.

(6) Develop procedures and techniques for installation and checkout.

(7) Define levels of responsibility for electronic security systems inspection, testing, and acceptance.

(8) Identify electronic security systems consulting sources for users.

(9) Determine electronic security systems inspection methods.

c. MACOM. The MACOM is responsible for forwarding requests for site surveys to the IDS–MCX and supporting it during site surveys. The MACOM establishes procedures for approval of requests for installation of electronic sécurity systems. The MACOM is responsible for providing funding for security site survey activities.

d. Installation commander. The installation commander identifies requirements for electronic security systems and initiates security site survey requests in accordance with MACOM procedures. The commander will brief the survey team on the local security threat, classification requirements, and prior physical security surveys and inspections. The commander will assign necessary personnel to assist the site survey team during the site survey.

e. Provost marshal inspection security officer. The provost marshal/installation security officer is the on-site representative in charge of security. He is responsible for final approval and acceptance of electronic security systems installations.

f. Director of Engineering and Housing (DEH). The DEH has the overall management responsibility for construction and maintenance of real property located on post.

C-3. Pre-Survey Requirements

a. Initiating a Site Survey. When the requirement of a site survey has been established in accordance with AR 190-13, a site survey support request letter will be prepared by the installation commander and sent to MACOM headquarters (fig C-1). It will include preliminary site survey information as shown in figure C-2, which will be used to plan and schedule the site survey. Pre-survey data will typically include—

(1) Facilities and/or resources to be protected.

(2) Protection required, based upon threat and applicable regulations.

(3) Description of existing electronic security systems.

(4) Previous survey documentation.

(5) Funding and schedule.

(6) Classification requirements.

(7) Existing physical security waivers.

b. Conducting site surveys. The MACOM has overall responsibility to conduct site surveys when requested by installation commanders. Depending upon the magnitude of the survey, the MACOM will request support from the IDS-MCX. After receiving a request for a survey, the IDS-MCX will conduct a "pre-survey" in order to develop a scope of work and cost estimate for the formal site survey.

c. Funding site surveys. The MACOM will fund the site survey, and furnish a completed site survey support request to the IDS-MCX.

d. Estimating the cost of the site survey. A cost estimate will be prepared to determine funding required. In order to properly estimate the cost of the site survey, it should be broken down into individual tasks,including types, numbers, and security requirements of individual facilities to be surveyed. The number of manhours to perform each task will be estimated, and a labor cost per manhour will be assigned, based upon who will be doing the work. Appropriate overhead, G&A, profit, travel, and other costs will be included in the total estimate. The completed cost estimate will be forwarded to the MACOM for funding. A site survey support request will not be forwarded to the IDS-MCX until MACOM program funds are available. If the cost estimate exceeds funds available by the MACOM, additional funds must be obtained, the scope of the site survey reduced, or the survey postponed until adequate funds are available. Paragraph C-8 of this appendix, "Estimating the Survey Costs," provides necessary guidance. Several factors will affect the cost of the site survey:

(1) Size and complexity of the site to be surveyed.

(2) Assets to be protected.

(3) Organization performing the site survey:

(*a*) On-site personnel.

(*b*) MACOM.

(*c*) IDS-MCX.

(*d*) Subcontractor.

e. Notification and Organization. After the site survey requirements have been established, a survey team chief will be selected to formulate and execute a site survey plan. The team chief will assemble the survey team. The functions and qualifications of potential survey team members are described in this guide. The survey team chief will send a survey notice to the site commander, provost marshal, and DEH, far enough in advance to allow site personnel time to collect required information and prepare for the survey. As a minimum, the survey notice will address the following topics:

(1) Survey schedule.

(2) Survey team members, including clearances.

(3) Facility access arrangements.

(4) Site specific information required, including:

(*a*) Master site plan or map;

(*b*) Prior security site survey documentation;

(*c*) Prioritized list of assets requiring protection;

(*d*) Current site security system;

(*e*) Current and potential threat analysis;

(*f*) As-built construction drawings;

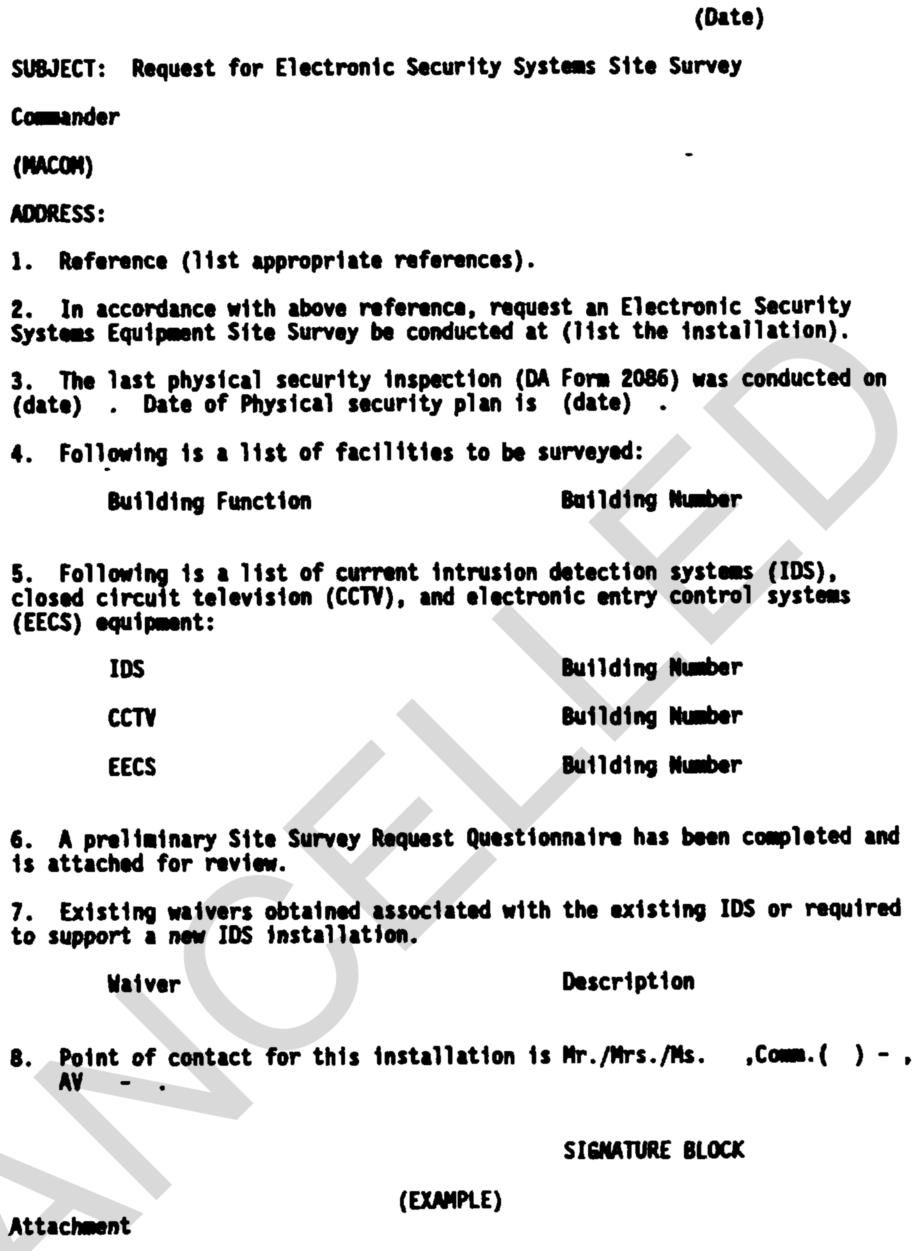
(*g*) Communications line drawings;

(*h*) Site electrical distribution;

(*i*) Security, safety, and fire regulations;

(*j*) Existing electronic security systems drawings and documents.

f. Site security clearance. Care will be taken during on-site activities and during information-gathering to observe all applicable security restrictions. Any classified information gathered during the survey will be safeguarded appropriately.



(Date)

SUBJECT: Request for Electronic Security Systems Site Survey

Commander

(MACOM)

ADDRESS:

1. Reference (list appropriate references).

2. In accordance with above reference, request an Electronic Security Systems Equipment Site Survey be conducted at (list the installation).

3. The last physical security inspection (DA Form 2086) was conducted on (date) . Date of Physical security plan is (date) .

4. Following is a list of facilities to be surveyed:

Building Function	Building Number

5. Following is a list of current intrusion detection systems (IDS), closed circuit television (CCTV), and electronic entry control systems (EECS) equipment:

IDS	Building Number
CCTV	Building Number
EECS	Building Number

6. A preliminary Site Survey Request Questionnaire has been completed and is attached for review.

7. Existing waivers obtained associated with the existing IDS or required to support a new IDS installation.

Waiver	Description

8. Point of contact for this installation is Mr./Mrs./Ms. ,Comm.( ) - , AV - .

SIGNATURE BLOCK

(EXAMPLE)

Attachment

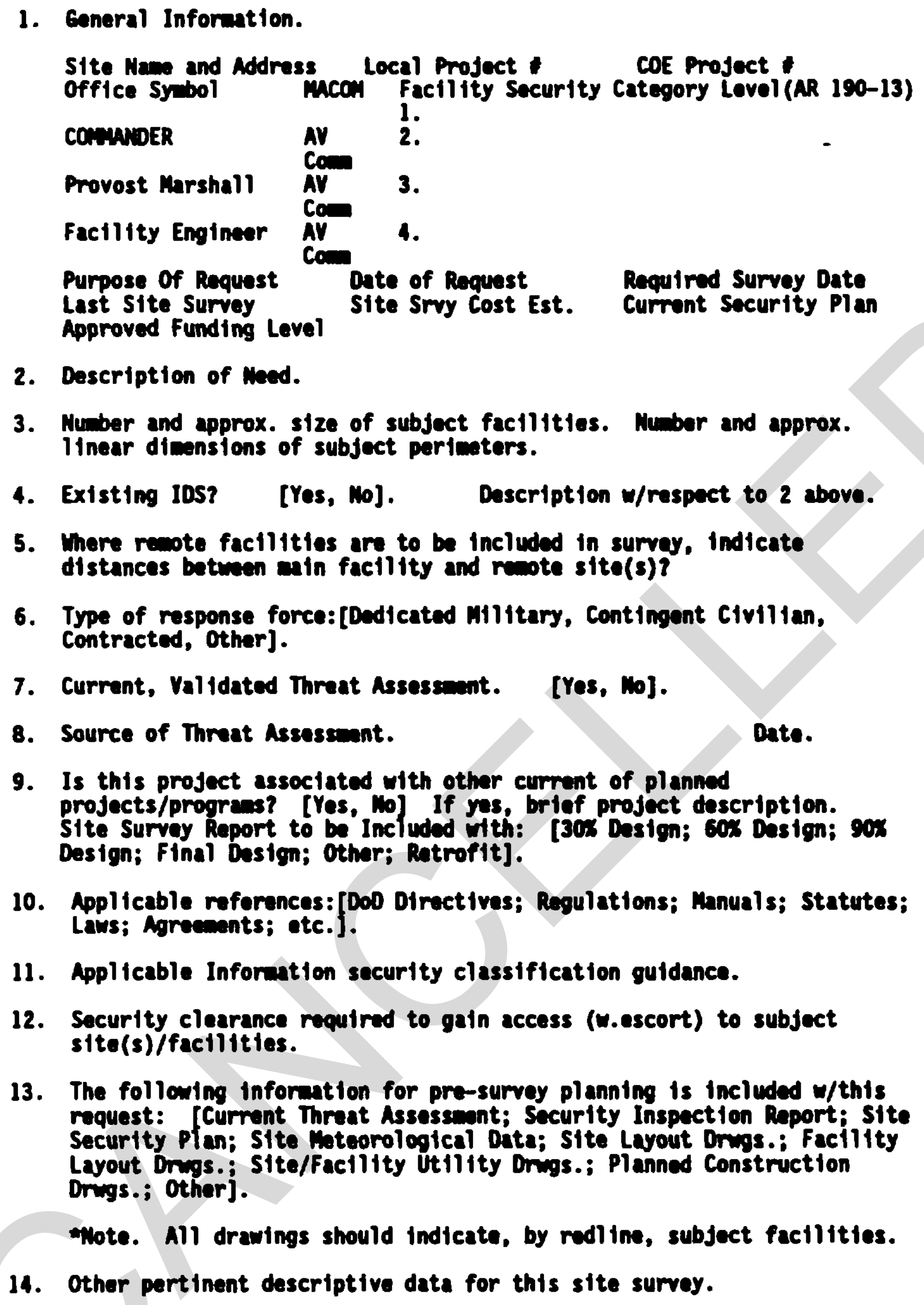
Figure C-1. Site Survey Support Request

Team members will have appropriate classification levels required by the installation and will be familiar with AR 380-5 and DOD 5200.1-R.

C-4. Site Survey Procedures

a. Organization of the Site Survey Team. The composition and size of the site survey team will be tailored to meet requirements dictated by size and complexity of the survey. A survey team will typically consist of two to four members. Team members will have expertise in electronics engineering, civil/structural engineering, communications engineering, security systems engineering, and safety engineering. Site support personnel with similar qualifications, if available, should be chosen to represent the site.

b. Survey team chief. The survey team chief will be the senior security specialist from the IDS—MCX or a security specialist from the MACOM of the installation to be surveyed, depending on who performs the survey. If the survey is to be done by a subcontractor, the team chief will be an individ-



1. General Information.

Site Name and Address   Local Project #   COE Project #
Office Symbol   MACOM   Facility Security Category Level(AR 190-13)

		1.
COMMANDER	AV Comm	2.
Provost Marshall	AV Comm	3.
Facility Engineer	AV Comm	4.

Purpose Of Request	Date of Request	Required Survey Date
Last Site Survey	Site Srvy Cost Est.	Current Security Plan
Approved Funding Level		

2. Description of Need.

3. Number and approx. size of subject facilities. Number and approx. linear dimensions of subject perimeters.

4. Existing IDS? [Yes, No]. Description w/respect to 2 above.

5. Where remote facilities are to be included in survey, indicate distances between main facility and remote site(s)?

6. Type of response force:[Dedicated Military, Contingent Civilian, Contracted, Other].

7. Current, Validated Threat Assessment. [Yes, No].

8. Source of Threat Assessment. Date.

9. Is this project associated with other current of planned projects/programs? [Yes, No] If yes, brief project description. Site Survey Report to be Included with: [30% Design; 60% Design; 90% Design; Final Design; Other; Retrofit].

10. Applicable references:[DoD Directives; Regulations; Manuals; Statutes; Laws; Agreements; etc.].

11. Applicable Information security classification guidance.

12. Security clearance required to gain access (w.escort) to subject site(s)/facilities.

13. The following information for pre-survey planning is included w/this request: [Current Threat Assessment; Security Inspection Report; Site Security Plan; Site Meteorological Data; Site Layout Drwgs.; Facility Layout Drwgs.; Site/Facility Utility Drwgs.; Planned Construction Drwgs.; Other].

*Note. All drawings should indicate, by redline, subject facilities.

14. Other pertinent descriptive data for this site survey.

Figure C-2. Preliminary Site Survey Information.

ual with expertise comparable to those above. The team chief will be experienced in—

(1) Electronic security systems selection, design, installation, operation, and maintenance.

(2) communications requirements for security systems.

(3) Physical security procedures.

(4) DOD security system regulations.

(5) Survey team leadership and coordination. The team chief will direct and coordinate all survey activities and interface with site personnel as required to accomplish the site survey. The team chief's responsibilities include—

(6) Sending the survey notice.

(7) Assemble the survey team.

(8) Organize and schedules the site survey.

(9) Handle survey team logistics.

(10) Conduct briefings.

(11) Develop and coordinates the site requirements letter.

c. Other team members. Team members will have the expertise to accomplish work required by the scope of the site survey. Depending upon the size of the survey team, individual members may fulfill more than one of the above categories, provided they have sufficient expertise. Team members will include specialists in any or all of the following areas:

(1) *Security systems.* Security systems require a knowledge and understanding of the application, installation, and operation of these systems.

(2) *Communications.* Communications includes testing, upgrading, and quality control of electronic security systems communications. Knowledge of these communications requirements and capabilities, including fiber optics and wirelines hardware and communications techniques, testing, physical security of communications equipment, installation, and operation is required.

(3) *Facilities engineering.* Facilities engineering includes all supporting engineering, installation, and construction logistics. An electrical background and experience in electronic security systems installation requirements, construction drawings, and power wiring diagrams is required.

(4) *Site engineering.* Site engineering includes civil/structural aspects of the survey. Familiarity with site plans, topographic maps and drawings, construction techniques, and structural limitations affecting electronic security systems installation is required.

(5) *Safety engineering.* Safety engineering requires a knowledge of electrical installation and National Electrical Code (NEC), particularly article 500, "Hazardous Classifications of Ammunition and Ammunition Storage," and knowledge of all safety regulations applicable to the site.

d. Video recording and photography. A VHS video camcorder and 35mm still camera will be used during site surveys to collect data to be used later in generating the report and design. Information regarding restrictions to the usage of cameras on site must be obtained ahead of time, and any special arrangements must be made. The following method of systematically videotaping and photographing a site will be used. An "outward-in" approach to videotaping will be used. Videotaping will start with the site's surroundings, move to the exterior of the structure, enter the structure, move to a specific location within the structure, go inside the specific location, and finally record the security details within the specific location. The following detailed step-by-step procedure assumes the target of the recording is a single building on the overall site being surveyed, and within this builidng there is a single room of interest. The following is the required step-by-step approach:

(1) Upon reaching the specific building to be surveyed, the camera operator will videotape the front of the building. A title board will be composed and held up to the camera at the start of the filming. The operator will state the compass heading while facing the building. The building will be slowly panned, taking care to stop on the building number and/or name and read them out loud to be recorded. After videotaping the front, the pan will be continued until a complete 360 degree view has been recorded. To ensure adequate sound fidelity, all narrating will be done by the camera operator. The still camera operator will also photograph the front of the building and surrounding area.

(2) After filming the front of the building, the camera operators will circle the building in a clockwise manner, stopping on each side and filming that side and surrounding area. All possible penetration paths into the facility will be recorded. Only after the entire exterior has been completed will the team move inside.

(3) When the team reaches the entrance to the room to be surveyed, a slow pan will be taken while standing in the center of the hall, centered on the room's door. This pan will include approaches to the room. Verbal comments will be made while videotaping. As a minimum the operator will identify the room.

(4) The team will next enter the room to be surveyed. A slow pan will be taken of the entire room from the door. This will make it easier later to locate highlight shots taken in the room.

(5) Detail shots will now be taken within the room. These shots will include sensor locations, CCTV equipment locations, other electronic security equipment locations, physical security features, the taking of the equipment location measurements, etc.

(6) Before moving on to the next site, the team will interview the person responsible for the space just surveyed, to gather additional data on the effectiveness of the existing system. The interview may be documented using video/audio taping or note taking.

(7) A team member with a 35 mm still camera will follow the video operator taking photographs in the same basic manner. Ample photographs will be taken to provide, along with the videotaping, a record of the facilities being surveyed. A high-quality 35 mm camera with ASA 400 speed color film and a 35 mm to 70 mm zoom lens is recommended.

C–5. Site Survey

a. Entrance briefing. An entrance briefing will be held on the first day of the survey. The briefing will be chaired by the survey team chief. It will include all survey team members and all applicable on-side personnel. The team will brief on-site personnel on objectives of the survey, information to be gathered, and procedures to be followed. The installation commander or his representative will brief specific site requirements, specific information about the installation, the mission, assets to be protected, and any security requirements to be observed. The on-site representatives should describe the existing security system and its operation.

b. Site survey guidelines. Site survey guidelines will be used during the on-site data gathering process as a guide to survey procedures and as a format for recording the data gathered. Paragraph C–7 of this appendix, "Survey Guidelines," contains a checklist to be used. Information will be added to or deleted, depending upon requirements of the survey. The guidance outline systematic recording of gathered data, which will be used with video tapes and photographs to provide a permanent record upon which the site survey report will be based.

(1) *Threat summary.* The threat summary will include information on generic and specific threats to the installation and its mission, vulnerabilities, history of prior incidences of this and similar facilities, potential adversaries, and existing conditions.

(2) *Exterior intrusion detection.* The exterior IDS section will describe existing exterior sensors, their locations, and existing site conditions in the vicinity where exterior IDS will be required. Physical conditions of the surrounding environment, meteorological conditions, and other exterior parameters will be described.

(3) *Facility description and interior intrusion detection.* The interior IDS section will describe existing interior sensors, their locations, and individual buildings and locations where interior IDS will be required. Physical conditions affecting the installation will be summarized, and space utilization, mission, mechanical and electrical equipment, and other information will be listed. Types and locations of doors, windows/portals, and sensors will be tabulated.

(4) *Surveillance and assessment.* Conditions involving CCTV, security lighting, and other surveillance and assessment activities will be noted. Security lighting requirements will be tabulated.

(5) *Perimeter barriers.* The perimeter fence or fences will be assessed by the team walking the perimeter, noting the type of fence, condition and location of gates, culverts, drains, utilities crossing the fence, nearby construction, and condition of the sills. Physical attributes for each section of the fence will be tabulated and located by reference to numbered light poles when possible.

(6) *Electronic entry control procedures.* Existing electronic entry control procedures will be assessed. The types of entry control used and proposed will be listed, including biometric devices, controlled portals, electronic or manual search aids, badging, card entry sytems, key and lock control, safes, and central entry control systems. Facility entry portals and their features will be tabulated. Windows and other non-entry portals will be tabulated.

(7) *Security systems communications.* Existing and proposed communications facilities and requirements will be summarized, including handheld and remote devices, telephone systems, exterior utilities, relay room, and other communication systems. Existing systems will be analyzed for their suitability to be used for security communications; however, it is noted that the communications media should be contractor furnished and installed with fiber optics as the preferred choice.

(8) *Facility power.* Existing and proposed facility power will be described, including types of power, stability, source, utility routes, and cable runs. Existing and proposed emergency power will be described, including types, capacity, response time, fuel type and location, and system usage.

(9) *Lighting to support CCTV assessment.* The survey team will measure the height of light poles, distance from the inner fence, light intensity, and note fixture types. The team will also measure and record details of light poles within 100 feet of a corner or line of site change in the fence and those in proximity to the Site Security Control Center.

(10) *Response.* The survey team will verify that adequate response force is available and will gather design-related criteria such as number of fixed posts, number of roving posts, and other relevant data.

(11) *Site-unique considerations.* Topological, geological, soil erosion, and other environmental conditions unique to the site, such as animal damage, will be assessed. Highways, secondary roads, railroads, waterways, and airways in the general vicinity will be listed.

c. Exit briefing. At the conclusion of the on-site phase of the survey, the survey team chief will conduct an exit briefing. Attendees at this briefing should be the same as at the entrance briefing. Preliminary findings, conclusions, and recommendations will be presented. Care will be taken to be factual and to avoid rendering decisions that may require additional study. The exit briefing will include a summary of any low cost, self-help suggestions that the installation could use to improve security.

C-6. Site Survey Report

a. Composition of the report. A site survey report will be prepared detailing the findings, conclusions, and recommendations resulting from the survey. The report will address the physical environment, facilities, existing IDS, and performance characteristics of the existing IDS. Detailed recommendations regarding revisions to the existing IDS and installation of new IDS will be included. Following is a typical table of contents:

(1) *Introduction.* The introduction will include the date of the survey, facility surveyed, mission or purpose, personnel in charge, and an overview of the survey.

(2) *Purpose of the report.* This section will give a brief desciption of the purpose of the report, which is to describe the site survey and methodology employed, and present the findings, conclusions, and recommendations resulting from the survey.

(3) *Survey team composition.* This section will list the team members, their qualifications, the team leader, and point of contact.

(4) *Security requirements.* This section will list specific security and clearance requirements of the facility, tenants, and/or missions; information to be safeguarded; and any other security considerations.

(5) *Sequence of events.* This section will describe the sequence of events that comprised the survey.

(6) *Facility tour.* This section will describe the facility tour that was performed, including building numbers, rooms, assets surveyed, fences and outlying facilities, and so forth.

(7) *Findings.*

(*a*) *Site description.* This section will include the MACOM, major tenants, mission, facilities and structures, and so forth.

(*b*) *Threat description.* This section will include a description of all real and potential threats.

(*c*) *Existing protection description.* This section will describe existing IDS and other protection in effect at the site.

(8) *Vulnerability analysis.* This section will address the vulnerability of the site based upon a comparison of the existing threat and the existing protection.

(9) *Design criteria.* This section will address the design criteria, in accordance with paragraph *c* below, "Threat analysis". It will include—

(*a*) Basis of design.

(*b*) Design alternatives.

(*c*) Drawings and sketches.

(*d*) Cost estimate.

b. Risk management. Risk management is the process of planning that allows the reduction of the probability and severity of loss or injury. Risk management, as applies to security protection, is usually done in three phases. These phases include the threat analysis, the vulnerability analysis, and the candidate system selection analysis. The first two phases are generally recognized within the security community. However, the later phase may also be referred to as the design criteria phase.

c. Threat analysis.

(1) The threat analysis consists of defining all of the variations of adverse occurrences that could occur. The following factors must be considered for each set of threat conditions:

(*a*) The person or group involved in the threat and their characteristics.

(*b*) The action involved in the threat.

(*c*) The asset to be protected.

(*d*) The severity of the success of the threat on the asset.

(2) Additional factors influencing the threat analysis include the determination of probabilities such as—

(*a*) Probability that the threat will occur.

(*b*) Probability that the action involved in the threat will be successful.

(*c*) Probability that the person involved in the threat will use deadly force.

(*d*) Quantified adverse impact resulting from threat success.

(3) In many cases, the Government has provided generic threat conclusions for security planners to work with. Even when these data are provided, the security planner must determine that all assumptions made in the generic threat still remain viable.

d. Vulnerability analysis. The security protection vulnerability analysis may be defined as the difference between existing security protective measures, if any, and the required protective measures. Hence, the vulnerability analysis deals with site-specific data. The security planner uses the results of the threat analysis (or provided statement of threat) and determines what vulnerabilities exist at the location to be protected. Vulnerabilities may be considered in a separate analysis or incorporated as part of the description of existing systems depending on the requirements of the evaluation process. Factors influencing the vulnerability analysis include—

(1) Barrier systems and delays.

(2) Electronic security systems.

(3) Response force capability and training.

(4) Security procedures.

(5) Installation security objectives.

e. Candidate system analysis.

(1) The candidate system analysis consists of listing possible ways of reducing various threats and vulnerabilities by implementing countermeasures. The candidate system analysis must consider the following factors:

(*a*) Countermeasure cost.

(*b*) Countermeasure effectiveness.

(*c*) Synergism between countermeasures.

(*d*) Regulatory mandated countermeasures.

It is helpful to consider how risk can be dealt with. The essence of risk management can be capsulized in the following three, and only three, actions that can be taken in response to a risk, either individually or in combination.

(*a*) *Preventative action.* Steps taken to prevent the threatened adverse occurrence from happening.

(*b*) *Contingent action.* Steps taken to reduce the adverse effects of a threatened adverse occurrence if it happens, regardless of the existence or absence of preventative measures.

(*c*) *Accept the risk (no special action).* If this action (or lack of action) is taken, then the loss is accpted if an adverse occurrence happens.

f. Design criteria. The design criteria will be of sufficient detail to show the overall concept of the intended system. It will provide a basis for final design and will include a cost estimate for funding and planning requirements. The design criteria will be included as a part of the site survey report and will include the following elements:

(1) A basis of design, which will be a generic description of the IDS to be used. The description will be of sufficient detail to allow a meaningful evaluation and will be the basis for the project cost estimate.

(2) A listing of any design alternatives that may be feasible to incorporate into the basis of design. The respective cost and features of each alternative should be listed, along with recommendations of specific alternatives and justification for their selection.

(3) Drawings and sketches, which will include the following:

(*a*) Block diagrams.

(*b*) Sensor and system location and details.

(*c*) Site plan.

(*d*) Typical cross-sections for fences.

(*e*) Floor plans.

(*f*) Specific sensor layouts.

(4) A project cost estimate of sufficient accuracy, which will be used for appropriations of funds and for planning purposes.

g. Survey report format.- The site survey report will consist of three volumes and will conform to the following format:

(1) Volume I.

(*a*) The basic report as decribed in the paragraphs above.

(*b*) Appendix A will consist of a tabulation of all IDS zones.

(*c*) Appendix B will consist of site plans and floor plans of all facilities covered in the survey.

(2) Volume II.

(*a*) Appendix C will consist of the threat statement as provided by the site requesting the survey. The appendix will be classified in accordance with applicable classification guides and AR 380–5.

(*b*) Appendix D will consist of the site deficiencies and vulnerabilities determined by the site survey. The appendix will be classified in accordance with applicable classification guides and AR 380–5.

(3) Volume III.

(*a*) Appendix E, which will be the cost estimate as described in paragraph C–8 of this appendix.

(*b*) The cost estimate will be designated "For Official Use Only."

C–7. Survey Guidelines

a. Purpose. The purpose of this survey guidance is to provide a list of important items to be investigated and to provide a uniform format for the recording of data gathered during an IDS survey. The information gathered is the data required to proceed with final design of the required IDS.

b. Complexity of site survey. Since the magnitude of scope of site surveys will vary, this may be added to or deleted from in tailoring it to requirements of the specific project. Applicable directives and guidance referred to in the guidelines will be followed when revising it.

c. Classified information. Specific classification requirements of the site to be surveyed will be established and strictly observed. Survey team personnel will be cleared at the appropriate classification levels and will be familiar with all applicable classification requirements. Any classified information gathered during this site survey will be safeguarded in strict accordance with applicable security regulations.

d. Pre-survey information.

(1) Is the Site Survey Request Questionnaire completed and attached as the first page of guidelines? Note discrepancies for on-site resolution.

(2) Is the information package (drawings, topographical map, site map, site plan drawing, site survey plan, security inspection report, meteorological data, and so forth complete? Note discrepancies for on-site resolution.

(3) Name of facility and location.

(4) Building ownership [Government-owned, leased from].

(5) Other tenants [Yes, No]. Describe.

(6) General workmanship/condition.

(7) Near-term modifications planned.

(8) Will modifications impact IDS [Yes, No]? Describe.

(9) Mission/purpose of facility.

(10) Facility sensitivity/criticality.

(11) Has the Site Survey Team been assembled [Yes, No] [name, organization, specialty, available date, contact number]?

(12) Has the Site Survey Notice been prepared? Include [schedule dates, team member clearance information, agenda, on-site documentation requirements, required interview, travel and lodging requirements/accommodations].

(13) Is coordination with the subject site complete? Note discrepancies for on-site resolution.

(14) In-briefing: One team member has been assigned to collect an attendance roster (name, title, organization and contact number) and to keep in-briefing minutes, to include site personnel briefing of requirements, current security system operations and procedures, and so forth. Furnish the name of team member.

(15) Site Survey Team facility tour: All team mebers should be guided through the site and should keep comprehensive notes for follow-on interviews and end-of-day team meetings.

(16) Potential Site Survey Equipment list: Include [Video tape recorder (VHS); video camera; 35 mm (SLR) still camera; TEMPEST-approved laptop computer; time domain reflectometer; optical time domain reflectometer; fiber optic signal source; fiber optic power meter; ground conductivity meter; soil conductivity test set; broad band spectrum analyzer; video test signal generator; oscilloscope; waveform monitor; digial BIT error rate detector; field strength meter; megger; dummy loads; wattmeter; sound level meter; footcandle meter; Brunton pocket transit; measuring devices (two 120' long x 1" wide tape measures; two 60' long x 1" wide tape measures; measuring wheel; visual range finder); and micro-cassette audio recorder].

e. Threat summary.

(1) Generic threats inherent in facility misson/function. Describe manmade threats, natural phenomena, or accidental events.

(2) Known vulnerabilities to specific threats.

(3) Have facilites of this nature been victimized elsewhere in this region [Yes, No]? If yes, explain cause/consequence.

(4) Predictors of potential threats: current reports or intelligence that this or similar facilities may be target of overt or covert activities.

(5) Indicate capabilities of potential adversary groups/individuals.

(6) Potential threat objectives on site.

(7) Are key individuals or functions located behind windows that are observable from the exterior of the facility?

(8) Actual events at this location [event, date, consequences].

(9) General comments.

f. Exterior intrusion detection.

(1) Note any sharp corners in the perimeter fence or roads.

(2) Could signs loosely mounted to the fence rattle and cause alarms (sensors)?

(3) What type of soil is between the fences (sandy, rocky, clay, and so forth; check each leg of perimeter)?

(4) What is topography between fences and in CCTV zones (level, uneven, depression, obstructions)?

(5) Is the soil stable or eroding? Erosion rate.

(6) Will grading be required (note areas)?

(7) Does terrain slope into fence or away? Are there culverts running through the perimeter fence?

(8) Are there utilities running through the perimeter fence [Yes, No]? Describe location/type [electrical, gas, sewer, telephone, other].

(9) Are there (inductive) machines nearby that could cause nuisance alarms [sewer lifts, pumphouses, welding shops, quarries with excavating machines, air conditioning equipment, water pumps, oil pumps, and so forth]?

(10) Are there any roads close to perimeter fences (give distance and location)?

(11) Are there any major highways close to perimeter fences (give distance and location)?

(12) Are there any railroad tracks close to perimeter (how often used)?

(13) Is any airport runway, landing pattern, or flight path close to the area?

(14) Where are likely places an intruder might attempt to penetrate the fence?

(15) Are any ground radar sites close to the area (distance/location)?

(16) Are any TV, radio, or microwave stations nearby (distance/location)?

(17) Are there any shipping installations close to the area (harbors, canals, channels)? Indicate (distance/location).

(18) Are birds, burrowing animals, or vegetation that could cause alarms or damage indigenous to the area?

(19) What is average rainfall (number of inches) per month?

(20) Monthly extreme temperature range.

(21) How often does site have fog (number of days) per month?

(22) What are the extreme wind velocities (average peak velocity) per month?

(23) How often does it snow (number of inches) per month?

(24) How often does area have blizzard/ice storms [seldom, frequent, occasionally]?

(25) How deep is frost line?

g. Facility description and interior intrusion detection.

(1) Building construction general description [thickness/resistance (basement, first floor, upper floors, ceilings, interior walls, other); to penetration (basement, first floors, upper floors, ceilings, interior walls, other)].

(2) Date constructed. By whom?

(3) Annunciator system [Yes, No]. Describe.

(4) Mechanical equipment/electrical relay rooms [Yes, No]. Describe.

(5) Telephone switching room [Yes, No]. Describe.

(6) Any special processes performed at this facility (chemical, nuclear, bacteriological) [Yes, No]? If yes, describe.

(7) Describe space utilization.

(8) Describe partitions [fixed, movable, combination].

(9) Compartmentalized interior [Yes, No]? If yes, explain.

(10) Are there any areas under CCTV surveillance [Yes, No]? If yes, give location.

(11) Are there any duress switches or silent alarm switches [Yes, No]? If yes, give type and location.

(12) Provide existing sensor type and locations.

(13) List doors with hinge type, location, description, striker type, and strength.

(14) Identify windows/utility portals (indicate all openings greater than 96 in^2).

h. Surveillance and assessment.

(1) Are sources of light or reflections located in the camera's field of view that will cause the camera's iris to close?

(2) Are CCTV zone images identified by zone number (zone marker or internal video processing system [Yes, No]? Describe.

(3) Will sunrise or sunset blind the cameras [Yes, No]? Describe.

(4) Would CCTV enhance perimeter IDS?

(5) How much [percent] of perimeter is under continuous observation by security force personnel?

(6) Is there enough light duirng day to support CCTV (consider weather)?

(7) At night do perimeter lights illuminate area enough to support CCTV (consider weather)?

(8) Identify areas where direct surveillance of CCTV assessment may be required to meet security lighting. Include (location, security operational requirements, and type effectiveness: distance and glare, photometer reading).

i. Perimeter barriers.

(1) Type of fence around area to be protected [single fence, double fence, chainlink, barbwire, and so forth].

(2) Condition of fence [loose, taut, sagging, base in concrete].

(3) Is fence high and secure enough for the anticipated threat?

(4) Does the fence have a sill to prevent tunnelling beneath? If so, describe.

(5) Are there gaps or washouts under the fence?

(6) Are there culverts or storm drains under the fence?

(7) Measure each leg of the fence and note here.

(8) Measure distance between fences (note variations).

(9) Measure distance between fence and structure(s) being protected.

(10) Are there any trees or structures near outside of fence [Yes, No]?

(11) Any materials or other items piled near inside of fence [Yes, No]?

(12) Any weeds or bushes growing along fence line [Yes, No]?

(13) Number and type of gates into protected area [locked and secure—no rattling; no unnecessary gates; securely mounted so they will not be easily removed; vehicle barriers]? If so, describe.

(14) Are there overhead utilities that could be used for entrance/exit [Yes, No]?

(15) Are there utility poles close to perimeter fence [Yes, No]?

(16) Are there electrical transformers close to perimeter fences [Yes, No]?

(17) Number of posts in each leg of fence [leg of fence, post number, type of post, height, diameter, composition].

j. Access control procedures.

(1) Will access control procedures include periodic subsystem testing and overall system evaluation [Yes, No]? Describe.

(2) Are biometric access control devices to be used [Yes, No]? If yes, describe.

(3) Is access to the base/installation controlled [Yes, No]? Describe.

(4) Is access to the activity controlled [Yes, No]?

(5) If portals are (or to be) manned, describe function of ECP officer.

(6) If portals are (or to be) covered by CCTV, describe viewing adequacy.

(7) Does each ECP have communications?

(8) For manned or machine-aided portals, what are estimated throughput rates by peak period(s) of use. (Key to portal number designation.)

(9) Are electronic or procedural search aids (to be) employed [Yes, No]? Describe.

(10) What design requirements exist for the access control subsystem [multiple access levels; fast throughput, area authorizations; time zoning, occupant listing, multi-man control, anti-passback, positive personal, identification, line security, expansion capability, other]?

(11) Describe barriers employed at each ECP; estimate penetration resistance.

(12) Are (employees, visitors) badged [Yes, No]? Do visitors sign-in [Yes, No]?

(13) Are badges color or otherwise coded for classification [Yes, No]? Describe.

(14) What controls are (or will be) employed for vehicle access to protected area(s)?

(15) How are blank badges controlled?

(16) Is a card access system used [Yes, No]? If yes, describe system.

(17) Designated emergency exits (indicate on floor plan).

(18) Will multi-man rules be employed [Yes, No]? If yes, in which areas.

(19) Describe entry/exit control procedures, expansion plans, current or anticipated problems, comments.

(20 Are key and lock combination controls in place [Yes, No]? If yes, describe.

(21) When was the last visual key audit made and by whom?

(22) Have losses occurred with no forcible entry?

(23) How often are locks and combinations changed?

(24) Are keys recovered when personnel leave [Yes, No]?

(25) Are duplicates (master, and so forth) stored securely [Yes, No]? Who has access?

(26) Who/where is locksmith?

(27) How are inventories or counts made on assets [frequency, responsibility, shortage reported, resolution]?

(28) General inventory (physical and procedural controls employed over other assets).

(29) Facility access controls (include exterior gates and doors and critical interior doors). Describe [portal number, location (N/S/E/W), function, frequency of use, type of control, resistance level (strength/duration), additional pertinent information].

(30) Windows/utility portals (indicate all openings greater than 96 sq in. where potential for forcible entry exists). Describe [locations, access from-to, penetration, resistance].

(31) Safes/Vaults [Location, access by, (physical/procedural) controls employed, (UL/GSA) rating, penetration resistance].

k. Security system communications.

(1) Are handheld or remote devices part of the communications system [yes, no]? If yes, give type and number.

(2) IDS and security telephone cable. Include as-built drawings (if available), EMI/RFI susceptibility; identify if cables can be jammed or covert monitored; are they encrypted?

(3) Are there utilities running through perimeter fence (note type/location) [electrical, gas, sewer, telephone, other]?

(4) Are there inductive machines nearby that could cause nuisance alarms?

(5) Telephone lines enter builiding where?

(6) List supplier and address.

(7) Relay room location(s) [relay room(s) secure, access controls] [Yes, No].

(8) Procedures for phone technician access.

(9) Indicate number of instruments on site and the number of lines.

(10) Land lines [Underground, poles, microwave, other].

(11) Data transmission in addition to voice [Yes, No].

(12) Describe other on-side communications.

(13) Is the telephone system proposed for alarm data communications from the protected area to the control point(s). [Yes, No] [if yes, will the control center be on or off-site; what is the condition/reliability of these telephone lines; will the use of these lines compromise facility security; what security countermeasures are to be applied to

these telecommunications; what alternatives will be developed]?

(14) If dedicated lease lines will be used, can line cost be reliably predicted for the life of the proposed system [Yes, No]? Source of cost data.

(15) Is there a redundant back-up system in the event of catastrophic failure of the primary system [Yes, No]? If yes, describe.

(16) What is the reliability of the primary system?

l. Facility power.

(1) Frequency of auxiliary power testing.

(2) Who supplies power to site?

(3) Location of nearest representative.

(4) Do power supply utilities run through or under perimeter fence [Yes, No]? If yes, describe below and note on site map.

(5) Where does power come onto site?

(6) How can this primary source be incapacitated?

(7) Type of primary power [1 Phase, 2 Phase, 3 Phase, 50Hz, 60Hz, 110v, 220v, other (specify)].

(8) Is power stable [Yes, No] [spikes, brownouts, other]?

(9) Cable runs [exposed, conduit, cable trays].

(10) Is there a source of emergency power on-site [Yes, No] [auto, manual]? If yes, describe [gas; diesel; battery; combination; capacity; manufacturer, location; are these areas secured?].

(11) Does system provide uninterruptible power [Yes, No]? If no, time to full capacity.

(12) Is IDS on uninterruptible or emergency power?

(13) What does system support?

(14) General comments.

m. Facility lighting.

(1) Are there perimeter lights (note type/location).

(2) Existing perimeter lights [Yes, No]? Indicate [type of lamps; wattage; illumination level; illumination uniformity; height of lamp; location of pole relative to fence or building; length of lamp support arm; distance between light poles].

(3) How are lights controlled [auto timer, photocell, manual]?

(4) Hours lights are on.

(5) How are light controls secured?

(6) Can lights be compromised easily?

(7) Are light fixtures vandal proof?

(8) Where do the lights receive their power?

(9) How can the lighting power source be incapacitated?

(10) Type of lighting power [1 Phase, 2 Phase, 3 Phase, 50Hz, 60Hz, 110v, 220v, other (specify)].

(11) Is there a source of emergency power for the lighting system [Yes, No] [auto; manual]? If yes, describe [gas; diesel, battery; combination; capacity; manufacturer; location; are these areas secured?].

(12) Does the emergency system provide uninterruptible power [Yes, No]? If no, time to full capacity.

(13) How often is the emergency power supply tested?

(14) General comments.

n. Response.

(1) Responsibility for facility security [name, telephone number, and so forth].

(2) How is response force activated?

(3) Total security complement [tours of duty (from-to), complement per tour (from-to)].

(4) Type of military security force [civilian, other] [supervision, training provided, turnover rate, selection criteria/qualifications].

(5) Principle functions/responsibilities (in rank order).

(6) Separately indicate the number of fixed posts and of mobile/roving posts.

(7) Ancillary functions.

(8) Are there written procedures [Yes, No]? If yes, how often are procedures updated?

(9) Limitation on new or revised functions.

(10) Organizational unit(s) responsible for electronic sensor maintenance [If none is available in-house, vendor(s) utilized; response time to call for service; general capabilities of vendor].

(11) Name of agencies with local police power/jurisdiction [agency location, complement, contact].

(12) General capabilities of agencies name above.

(13) Do any (all) agencies named above accept alarm devices [Yes, No]? If yes, give names and description of available services.

(14) Response time for agencies named above.

(15) If agencies are contacted, what problems/needs do they see for this site [population of local government, demographics, principal local problems impacting site]?

(16) Additional pertinent information.

(17) General comments.

(18) Response force equipment [type, quantity, location].

o. Site-unique considerations.

(1) Obtain topological map, site map and site plan drawing.

(21) Some sites may contain classified equipment or information. Site surveys for these sites should be carefully reviewed for classificaiton.

(3) Is there any history of seismic activity in this area [Yes, No]? Explain.

(4) Any history of/or special exposure to natural phenomenon [hurricane, forest fire; tidal

waves; tornadoes; volcano; lightning, extreme temperature, sandstorms, blizzards].

(5) Elevation above sea level.

(6) Proximity of site to major terrain features such as swamps, forest, sea coast, lakes, and so forth (give location/distance).

(7) Are there any major highways, secondary roads, railroad, waterways, or airways within 2 mi (3.2 km) of this site? Describe.

(8) The site map should provide detailed information concerning the following or it should be obtained during the site survey [location of all facilities to be considered in the survey, location of any planned or potential contruction].

(9) The site plan drawings should provide detailed information about the following or it should be obtained during the site survey [topographic details; drainage systems and water retaining features; natural or man-made barriers or places of concealment; detailed data for locations where proposed sensor system will be routed; identity locations of all internal and adjacent external road-ways; railroads, fences, and buildings; identify areas of programmed or potential future construction areas at the site; identify location, type and routes of all utilities crossing the sensor area; identify location and type for all existing security/communication systems, and components such as detection sensors, cameras, radios, and so forth; make special note of any malfunctioning or unused equipment (location, type, model, serial number].

(10) Describe any adjoining property [direction, owner, boundary, delineation].

(11) Have these properties been victimized [Yes, No]?

(12) Do these properties represent a threat [Yes, No]?

(13) How is access from these properties controlled [during normal duty hours; during off-duty hours]?

C-8. Estimating the Survey Costs

a. Purpose. The purpose of this section is to provide a standard methodology for estimating the cost of performing an IDS site survey. By breaking the survey process down and assigning manhours to each component, the system can be applied to surveys of any size.

b. Procedure. The sizes and types of facilities and their required security levels will be identified, and the estimated time to survey each will be picked from the recurrent hours matrix (table C-1). In addition, trips to various facilities will be included. Hours will be allocated for on-site time, survey report preparation time, and design criteria time. These will then be multiplied by the quantity of each type of facility being surveyed.

(1) Estimated time required to perform each nonrecurrent element will then be chosen from each appropriate column of the nonrecurrent hours matrix (table C-2). Items that do not fit into any of the categories listed will be estimated on an individual basis.

(2) The total number of labor hours estimated to perform the site survey is arrived at by adding the component hours. This total will be multiplied by the labor rates to be used, with appropriate fringes, overhead, and other costs being added. An example is shown in table C-3.

Table C-1 Recurrent Hours Matrix

Activity	Qty.	On-site Hours	Survey Report Hours	Design Criteria Hours	Total Hours
1. Perimeters[1]		2.0	4.0	25	
2. High Security Rooms[2]		2.0	20 0	20	
3 Low Security Rooms[2]		0 75	15.0	15	
4. Ammunition igloos[3]		0.75	17.0	17	
5 Trips to facilities[4]		0.25	0.0	0	
6 Key person interviews		1.0	0 5	0	

Notes.

1. Per 1,000 linear feet

2 Per each.

3. Per igloo. In large groups of igloos, not all igloos may have to be surveyed, only representative igloos or other specific igloos.

4 Per trip

Table C-2 Non-Recurrent Hours Matrix.

Activity	*Hours*
1. Survey Plan	32
2. Survey Notice	4
3. Prepare In-Briefing	4
4. Present In-Briefing	4
5. Background Information	32
6. Prepare Out-Briefing	4
7. Present Out-Briefing	4
8. Government Review	16
9. Report Revisions	32

Table C-3 Sample Estimated Survey Cost

Facility Description

* 20,000 foot perimeter fence
* 20 high security fence
* 30 low security rooms
* 30 ammo igloos; 4 different types
* 12 key person interviews
* 10 trips to facilities required

Recurrent Hours Matrix

Activity	*Qty*	*On-Site Hours*	*Survey Report Hours*	*Design Criteria Hours*	*Total Hours*
1. Perimeters[1]	20	2.0	4.0	25	620
2. High Security Rooms[2]	20	2.0	20.0	20	840
3. Low security Rooms[2]	30	0.75	15.0	15	922
4 Ammunition igloos[3]	4	0.75	17.0	17	139
5 Trips to facilities[4]	10	0.25	0.0	0	2
6 Key person interviews	12	1.0	0.5	0	18
				Subtotal	2,541

Non-Recurrent Hours Matrix

Activity		*Hours*
1. Survey Plan		32
2 Survey Notice		4
3 Prepare In-Briefing		4
4. Present In-Briefing		4
5. Background Information		32
6. Prepare Out-Briefing		4
7. Present Out-Briefing		4
8. Government Review		16
9 Report Revisions		32
	Subtotal	132
	Grand Total MH	2,673

Notes

1. Per 1,000 linear feet

2 Per each.

3. Per igloo. In large groups of igloos, not all igloos may have to be surveyed, only representative igloos or other specific igloos

4. Per trip.

BIBLIOGRAPHY

Books

Barnard, Robert L. *Intrusion Detection Systems*, 2nd ed. Massachusetts: Butterworth Publishers, 1988.

Bose, Keith W. *Video Security Systems*, 2nd ed. Massachusetts: Butterworth Publishers, 1982.

Bowers, Dan M. *Access Control and Personal Identification Systems*. Massachusetts: Butterworth Publishers, 1988.

Cherry, Don T. *Total Facility Control*. Massachusetts: Butterworth Publishers, 1986.

Fennelly, Lawrence J. *Handbook of Loss Prevention and Crime Prevention*, 2nd ed. Massachusetts: Butterworth Publishers, 1988.

Schnabolk, Charles. *Physical Security: Practices Plus or Minus Technology*. Massachusetts: Butterworth Publishers, 1983.

Walker, Philip. *Electronic Security Systems*, 2nd ed. Massachusetts: Butterworth Publishers, 1988.

Weber, Thad L. *Alarm Systems and Theft Prevention*, 2nd ed. Massachusetts: Butterworth Publishers, 1985.

Publications of Department of the Army, Huntsville Division, Corps of Engineers

Cost Estimating Guide for Intrusion Detection Systems.

Site Survey Procedures Guide for Intrusion Detection Systems.

CEGS–16725: Intrusion Detection System.

CEGS–16751: Closed Circuit Television Systems for IDS.

CEGS–16752: Electronic Entry Control Systems.

CEGS–16753: Wireline Data Transmission Media for Security Systems.

CEGS–16754: Fiber Optics Data Transmission Media for Security Systems.

HNDM–1110–1–1: Engineering Guidance Design Manual for Architect-Engineers.

HNDSP 85–112–ED–CS: Computer-Aided Design and Drafting (CADD) System Standard Operating Procedures.

Other Documentation

Sandia Laboratories, *Intrusion Detection Systems Handbook,* SAND76–5554.

Sandia Laboratories, *Entry-Control Systems Handbook,* SAND77–1033.

Sandia Laboratories, *Safeguards Control and Communication Systems Handbook,* SAND78–1785.

GLOSSARY

Abbreviations

ASCII	American Standard Code for Information Interchange
BISS	Base Installation Security System
BMS	Balanced magnetic switch
CCD	Charge coupled device
CCTV	Closed circuit television
DTM	Data transmission media
EECS	Electronic entry control system
EMI	Electromagnetic interference
FAR	False alarm rate
FCC	Federal Communication Commission
FIEPSS	Fixed Installation Exterior Perimeter Sensor System
FOV	Field of view
GFE	Government furnished equipment
HVAC	Heating, ventilating, and air conditioning
ICIDS	Integrated Commercial Intrusion Detection System
IDS	Intrusion detection system
IR	Infrared
ISIT	Intensified silicon intensifier target
J–SIIDS	Joint-Service Interior Intrusion Detection System
LED	Light-emitting diode
MTBF	Mean-time-between-failure
MTTR	Mean-time-to-repair
NAR	Nuisance alarm rate
NFPA	National Fire Protection Association
PIN	Personal identification number
PIR	Passive infrared sensor
PTZ	Pan, tilt, and zoom
RAM	Random access memory
REMBASS	Remotely Monitored Battlefield Sensor System
RF	Radio frequency
RFI	Radio frequency interference
ROM	Read-only member
SCIF	Sensitive compartmented information facility
SIT	Silicon intensifier target
UL	Underwriters Laboratories
UPS	Uninterruptible power supply

The proponent agency of this publication is the Office of the Chief of Engineers, United States Army. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to HQUSACE (CEMP-ET), WASH DC 20314-1000.

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:

Milton H. Hamilton

MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

Distribution:

Army: To be distributed in accordance with DA Form 12-34-E, Block 4506, requirements for TM 5-853-4.

*U.S. G.P.O.:1994-300-723:80114