UFC 4-021-02NF
27 September 2006
change 1, 23 October 2006

# UNIFIED FACILITIES CRITERIA (UFC)

## SECURITY ENGINEERING

## ELECTRONIC SECURITY SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

UFC 4-021-02NF
27 September 2006
change 1, 23 October 2006

# UNIFIED FACILITIES CRITERIA (UFC)

# ELECTRONIC SECURITY SYSTEMS

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER SUPPORT AGENCY

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

| **Change No.** | **Date** | **Location** |
|---|---|---|
| 1 | 23 Oct 06 | Title adjusted |

## FOREWORD

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 Civil Engineer Support Agency (AFCESA) 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.

AUTHORIZED BY:

| | |
|---|---|
| | James Wright |
| DONALD L. BASHAM, P.E.<br>Chief, Engineering and Construction<br>U.S. Army Corps of Engineers | DR. JAMES W WRIGHT, P.E.<br>Chief Engineer<br>Naval Facilities Engineering Command |
| Kathleen I. Ferguson | |
| KATHLEEN I. FERGUSON, P.E.<br>The Deputy Civil Engineer<br>DCS/Installations & Logistics<br>Department of the Air Force | Dr. GET W. MOY, P.E.<br>Director, Installations Requirements and Management<br>Office of the Deputy Under Secretary of Defense (Installations and Environment) |

## Unified Facilities Criteria (UFC)

## New Document Summary Sheet

**Subject:** UFC 4-021-02NF, Electronic Security Systems (ESS).

**Cancels:** This document replaces Navy Design Manual 13.02, Commercial Intrusion Detection Systems (IDS), September 1986.

**Description:** This UFC (Unified Facilities Criteria) document provides guidance on how to design electronic security systems required by the current antiterrorism/force-protection environment. Electronic security systems consist of access control systems (card reader systems), closed-circuit television (CCTV) system, intrusion detection systems, data transmission media systems (a means to communicate information internally and externally to DoD sites), and provision of local or regional dispatch centers (also known as security command centers). Electronic security systems are one part of an overall physical security plan. This document provides guidance to commanders, architects and engineers on how to design electronic security systems for projects to include new construction, additions, renovations, expeditionary, or temporary construction.

**Reasons for Development:**

Naval Facilities Engineering Command accepted responsibility of the Navy's Physical Security Equipment Program, including ESS in Oct 2004. The Navy's criteria for ESS is outdated (1986) and currently there is no Tri-Service Criteria for Electronic Security Systems. The Army is in the process of updating Army TM 5-853-04 (1994) for the Tri-Service, but finalization is not anticipated for another year. There have been significant technology advancements in field of Electronic Security Systems, especially in the areas of CCTV and access control. Therefore, the Navy has an emergent need for updated criteria. Since the schedule for the Tri-Service manual would not meet the immediate need, it was decided to publish a Navy only UFC. Once this UFC is published, the intent is to combine with the Army's update to create a Tri-Service UFC for ESS.

- This UFC is one of a series of new security engineering UFC documents covering physical countermeasures for the current threat environment.
- The design of electronic security systems is a specialized technical area that does not fall in the normal skill record and resume of commanders, architects, engineers and project managers. This UFC provides guidance to those parties tasked with implementing existing and emerging physical protection system requirements.

**Impact:** The following direct benefits will result from the publication of UFC 4-021-02N:

- Creation of a single source reference for the design and construction of electronic security systems.
- Implementation of automated, hardware electronic security systems will reduce costly labor-intensive security personnel forces.
- Provision of automated intrusion detection systems and methodologies enhance force protection vigilance by not relying on human operators, who are subject to monitoring fatigue.
- Cost savings through implementation guidance on how to consolidate diverse dispatch centers (security command centers) into regional dispatch centers.

- Reduced facility project costs and efficiencies achieved by a better-educated command, designer, and project management staff for the specialized technical area of electronic security systems.
- The modernized facilities will perform better in terms of force protection than they did originally.

**CONTENTS**

## Table of Figures and Tables

# CHAPTER 1

# INTRODUCTION

## 1-1 PURPOSE

The purpose of this UFC is to provide guidance for designing Electronic Security Systems (ESS) in support of the Department of Defense (DoD) physical security program requirements. An ESS is one of many physical security measures that must be considered when addressing the physical security posture of a facility. This UFC is intended to provide uniformity and consistency in the design of an ESS.

### 1-2.1 Applicability

This UFC provides planning and design criteria for DoD components and participating organizations. This UFC applies to all construction, renovation, or repair projects that include an Electronic Security System.

## 1-2 SCOPE

This UFC provides guidance in designing an ESS. It is not intended to create the requirement for an ESS, but rather to assist in designing systems that meet an established requirement and to give guidance to commanders, architects, and engineers on designing an ESS for new projects. Headquarters, Major Command, and installation physical security personnel should be consulted for DoD and Service directives outlining ESS requirements for asset protection. The ESS requirement may come from DoD standards, installation requirements, or user requirements. Projects may include new construction, additions, renovations, expeditionary, or temporary construction.

A vulnerability assessment must be conducted prior to beginning a security project (see the sections “Vulnerability Assessment—Identify Critical Assets” and “Vulnerability Assessment—Design Basis Threat (DBT)” in Chapter 2, “Electronic Security System Overview.” Having identified what facility or elements might be vulnerable to which threats, physical security measures such as an ESS can be implemented to reduce the risk of intrusion and subversive acts. In summary, this UFC assumes the pre-design phases, including the risk analysis, are completed prior to beginning ESS design. For information on design requirements, refer to UFC 4-020-01 and UFC 4-020-02 (described in the section “Security Engineering UFC Series” in this chapter).

## 1-3 REFERENCES

1-3.1 Appendix A contains a list of references used in this UFC. The publication date of the code or standard is not included in this UFC. In general, the latest available issuance of the reference was used.

## 1-4 GLOSSARY

Acronyms, abbreviations, and terms are defined in Appendix B.

## 1-5 SECURITY ENGINEERING UFC SERIES

1-5.1 This UFC is one of a series of security engineering UFC manuals that cover minimum standards, planning, preliminary design, and detailed design for security and antiterrorism. The documents in Series 4-0xx are designed to be used sequentially by a diverse audience to facilitate development of projects throughout the planning, design and acquisition cycle**.** The manuals in this series are identified in the following subsections.

1-5.2 **DoD Minimum Antiterrorism Standards for Buildings.** UFC 4-010-01 and UFC 4-010-02 (For Official Use Only—FOUO) establish standards that provide minimum levels of protection against terrorist attacks for the occupants of all DoD inhabited buildings. These UFCs are intended to be used by security and antiterrorism personnel and design teams to identify the minimum requirements that must be incorporated into the design of all new construction and major renovations of inhabited DoD buildings**.** They also include recommendations that should be, but are not required to be incorporated into all such buildings.

1-5.3 **Security Engineering Facilities Planning Manual.** UFC 4-020-01 (not published at the time of this printing) presents processes for developing the design criteria necessary to incorporate physical security and antiterrorism into DoD facilities and for identifying the cost implications of applying the design criteria**.** The design criteria may be limited to the requirements of the minimum standards, or they may include:

- Protection of assets (people) other than those addressed in the minimum standards
- Aggressor tactics that are not addressed in the minimum standards
- Levels of protection beyond those required by the minimum standards

The cost implications for physical security and antiterrorism are addressed as cost increases over conventional construction for common construction types. The changes in construction represented by the cost increases are tabulated for reference, but they cover only representative construction that meets the requirements of the design criteria. The manual also includes a means to assess the tradeoffs between cost and risk. The *Security Engineering Facilities Planning Manual* is intended to be used by planners as well as physical security and antiterrorism personnel with support from planning team members.

1-5.4 **Security Engineering Facilities Design Manual.** UFC 4-020-02 (not published at the time of this printing) provides interdisciplinary design guidance for developing preliminary protective measures systems to implement the design criteria established using UFC 4-020-01. Those protective measures include building and site elements, equipment, and the supporting manpower and procedures necessary to make them all work as a system. The information in UFC 4-020-02 is in sufficient detail to support concept-level project development and provides a sound basis for a more detailed design. This UFC also provides a process for assessing the impact of protective measures on risk. The primary audience for the "Security Engineering Facilities Design Manual" is the design team, which should include security (Physical Security Officer) and antiterrorism personnel. Security is an essential part of the design team and they should bring in antiterrorism personnel (Antiterrorism Officer ATO), when appropriate.

1-5.5 **Security Engineering Support Manuals.** In addition to the standards, planning, and design UFCs described above, there are additional UFCs that provide detailed guidance for developing final designs based on the preliminary designs developed using UFC 4-020-02. These support manuals provide specialized, discipline-specific design guidance. Some address specific tactics such as direct fire weapons, forced entry, or airborne contamination. Others address limited aspects of design such as resistance to progressive collapse or design of portions of buildings such as mailrooms. Still others address details of designs for specific protective measures such as vehicle barriers or fences. The *Security Engineering Support Manuals* are intended to be used by the design team during the development of final design packages. This UFC is one of the supporting manuals.

## 1-6 ORGANIZATION OF THIS UFC

1-6.1 Following this introductory chapter, the remaining chapters present information on how to design ESS subsystems as described in the next subsections.

1-6.2 **Chapter 2, Electronic Security Systems Overview** provides an overview of how ESS make up part of an overall physical security system solution. Information on the Detect, Delay, Respond principle is presented as well as a brief background on the vulnerability assessment process that precedes ESS design. Overview information is presented on system architectures, from simple to complex, and system monitoring methods. Additional specific information is provided for each subsystem in the subsequent chapters.

1-6.3 **Chapter 3, Access Control Systems**. An access control system (ACS) is a system that ensures only authorized personnel are permitted ingress into or egress from a controlled area. (Other DoD documents may refer to the ACS as an Automated Access Control System or an Electronic Entry Control System.) This chapter describes the elements of an ACS including card readers, common access card (CAC) credentials, biometric readers, electronic door locks, and the computer and electronic systems necessary to integrate these elements.

1-6.4 **Chapter 4, Closed Circuit Television Systems**. A closed circuit television (CCTV) system is the collection of cameras, video recorders, and other equipment that allows security events to be viewed, monitored, and recorded. This chapter covers the components of a CCTV system and the interface with the Dispatch Center.

1-6.5 **Chapter 5, Intrusion Detection Systems.** An intrusion detection system (IDS) is a system that detects the presence of intruders. This chapter discusses the elements of an IDS including sensors such as motion detectors, active and passive infrared sensors, cables designed to sense movement or pressure when buried underground, point alarms such as magnetic door switches, and glass breakage sensors. An IDS system requires integration with a process and mechanisms for assessing and responding to intrusion alarms.

1-6.6 **Chapter 6, Data Transmission Media.** The data transmission media (DTM) system transmits information from sensors, ACS devices, and CCTV components to display and assessment equipment. This chapter explains the significance of the DTM. A DTM is a communication path or network for transmission of data between two or more components, and back to the Dispatch Center.

1-6.7 **Chapter 7, Dispatch Center.** A Dispatch Center is the area containing the personnel and alarm notification equipment that monitor inputs from the ACS, IDS, CCTV, and communications systems. At the Dispatch Center, alarms are received, are assessed and response actions are initiated including dispatching as necessary. This chapter discusses the function and requirements of the Dispatch Center.

1-6.8 **Chapter 8, ESS Subsystem Integration.** Integration of the various subsystems for the ESS is discussed. Topics covered include communication from the ACS to door and gate hardware, IDS to ACS, ACS to and from the CCTV subsystem, and ACS to and from the Dispatch Center.

1-6.9 **Chapter 9, General Requirements and Cross-Discipline Coordination.** General considerations such as system acceptance testing, operation, and maintenance, architectural coordination issues and electrical coordination issues are discussed.

1-6.10 **Chapter 10, Model Design Approach.** To close this UFC, a chapter on a model ESS design approach is provided. This chapter does not mandate an approach but describes an effective model approach on how to design an ESS.

# CHAPTER 2

# ELECTRONIC SECURITY SYSTEM OVERVIEW

## 2-1 OVERVIEW

2-1.1 ESS is the integrated electronic system that encompasses the ACS, interior and exterior IDS, CCTV systems for assessment of alarm conditions, the DTM, alarm reporting systems for monitor, control, and display, and the policies, procedures, and response times that ensure that all elements of the ESS work effectively. It is part of an overall physical protection system. As shown in Figure 2-1, the overall physical protection system consists of civil engineering features of fences, gates, entry points, clear zones, and standoff distances; architectural issues of construction materials, barriers, doors, windows, and door hardware; structural issues of blast resistant protection; mechanical issues of HVAC protection, electrical engineering issues of power redundancy and lighting systems, ESS, and operational considerations such as policy, procedures, and response times . In summary, the ESS is one component of a bigger physical protection scheme. This chapter describes the ESS in general as a lead-in to subsequent detailed chapters on each of the ESS subsystems.

**Service Exception, Marine Corps**: Aboard Marine Corps Installations, Mass Notification Systems (MNS) are considered a component of the ESS. Design of Mass Notification Systems is not within the scope of this UFC, refer to UFC 4-020-01 for Mass Notification System design guidance.

## 2-2 DETECT, DELAY, AND RESPOND

2-2.1 For effective intrusion intervention, the ESS should operate on the Detect, Delay, and Respond principle that ensures the time between detection of an intrusion and response by security forces is less than the time it takes for damage or compromise of assets to occur. Refer to Figure 2-2. (Note: Some documents consider the additional specific steps of Annunciate, Classify, and Assess as part of the intrusion intervention process. These additional steps are part of the process, but for this document are intrinsically included as part of the Detect step.)

2-2.2 Table 2-1 provides an example of the times related to each detect and delay option in Figure 2-2. The cumulative delay times shown in this example, illustrated by a timeline in Figure 2-3 are estimated at slightly over eight and a half minutes. Assuming a security forces response time of eleven minutes, the sequence of events shown in Table 2-1 allows sufficient time for an adversary to compromise and/or damage the targeted asset. Depending on the nature of the asset, there are some dictated response times. Security and planning personnel should refer to DoD, agency, and service directives to identify response requirements.

2-2.3 Conversely, assuming a security forces response time of five minutes, the sequence of events shown in Table 2-1 allows sufficient time to intervene on the intrusion efforts**.** In designing an ESS, the designer should work with the facility/base security officer to identify the response forces and reaction times.

2-2.4 The above example is provided to illustrate the general principles of Detect, Delay, and Respond. Table 2-2 provides additional samples of Detect, Delay, and Respond factors. For additional information on delay times, refer to the book *The Design and Evaluation of Physical Protection Systems.*

**Figure 2-1. ESS as a Part of a Physical Security System**

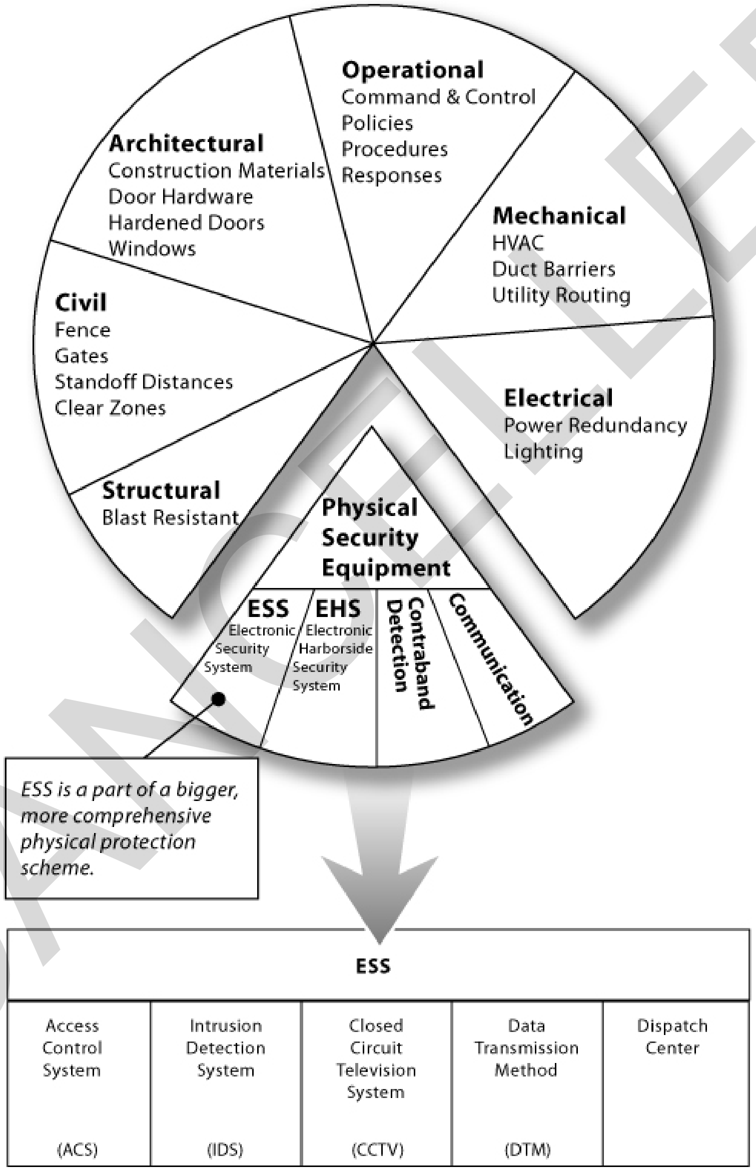


**Figure 2-2. Example Detect and Delay Options**

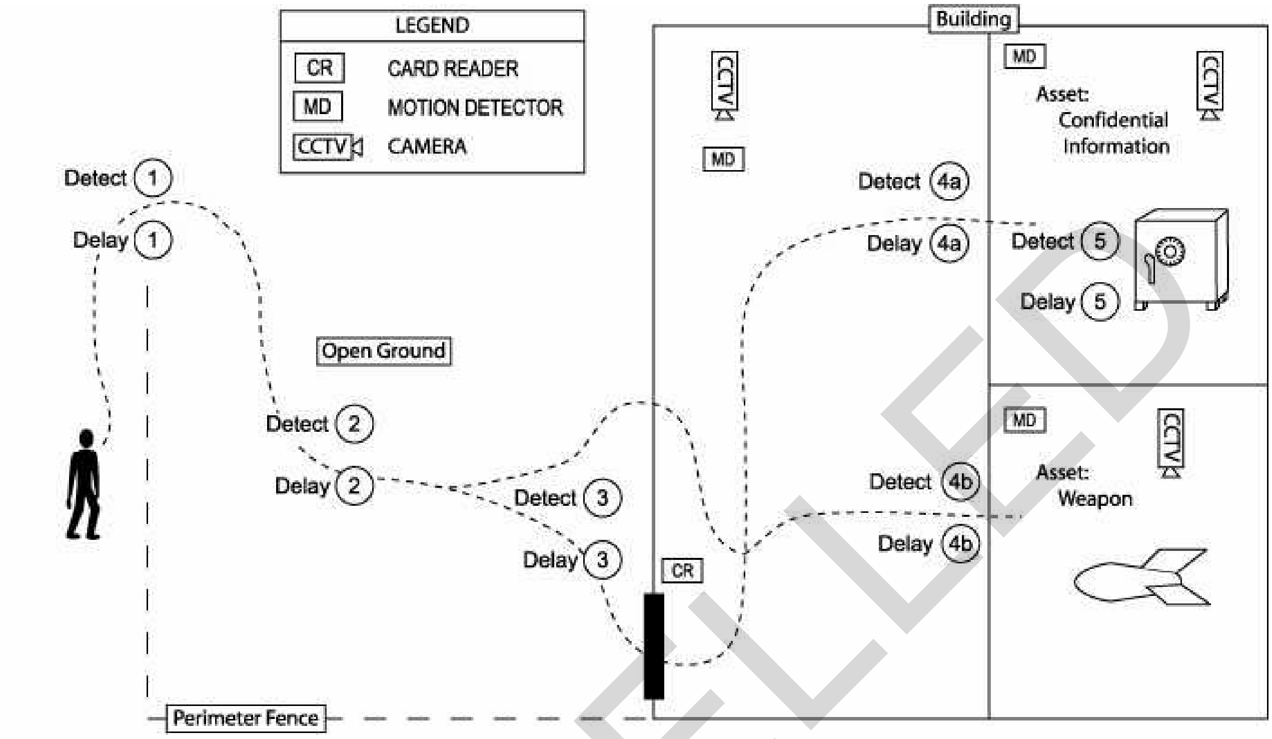


**Table 2-1. Example Breach Events and Delay Time**

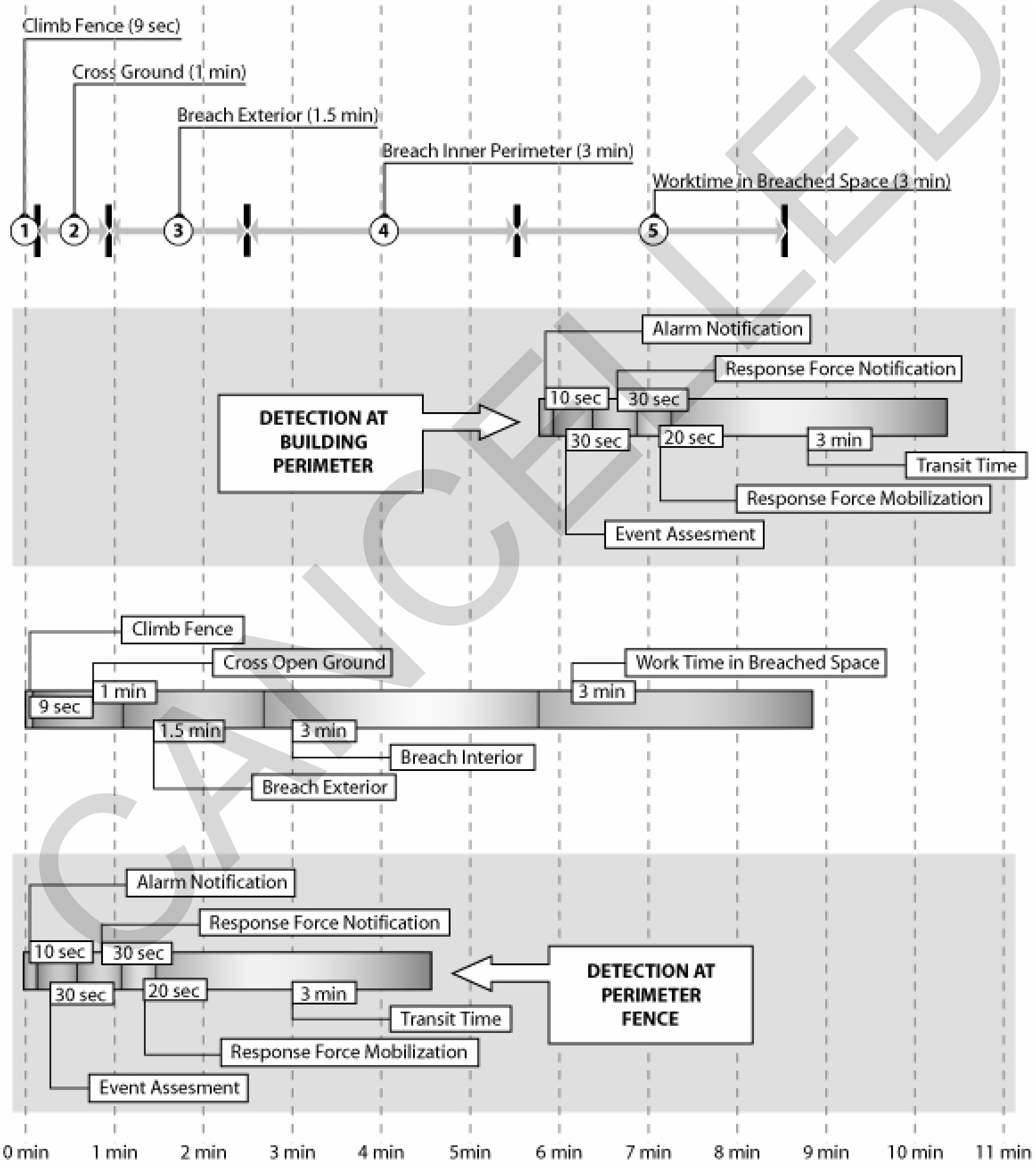
| | Delay Options | Delay Time | Detection Options |
|---|---|---|---|
| **1** | Climb fence | 8-10 sec. | Perimeter fence detection system |
| **2** | Cross open ground | 10 feet/sec. | Microwave sensors |
| **3** | Breach building door or window or wall | 1-2 min. | Door contacts or glass breakage sensor |
| **4** | Breach interior hardened door | 2-4 min. | Door contacts |
| **5** | Work time in breached space | 3 min. | Motion sensor |
| **TOTAL DELAY TIME** | | 8 min 39 sec nominal for this example | |

**Table 2-2. Sample Detect, Delay, and Respond Measures**

| Detect Measures | Delay Measures | Respond Measures |
|---|---|---|
| Intrusion detection devices | Fences | Response force alerted |
| Alarm notification | Walls | Response force travel |
| Visual displays | Doors | Neutralization |

2-2.5 Figure 2-3 shows two cases of alerting a response force. In the first case, initial detection is not made until the interior wall of the critical asset has been breached. With initial detection at six minutes, response forces do not arrive on the scene until after some compromise of the critical asset has been achieved. In the second case, initial detection is made at the fence line and allows response forces to arrive and intervene before asset compromise.

**Figure 2-3. Timeline Showing Two Cases of Breach and Detection**



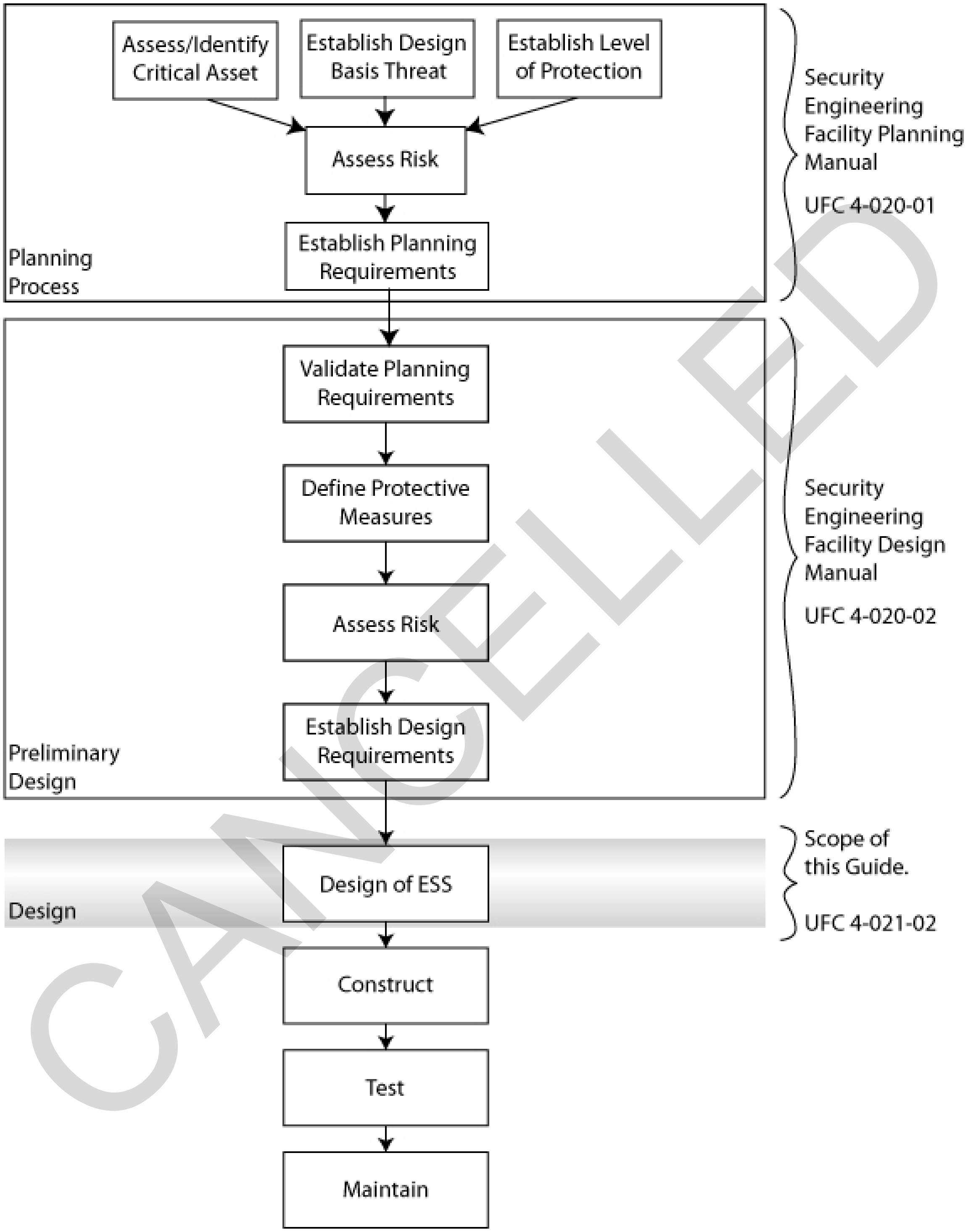
In the above timeline, there will be a difference in time required to provide protection depending on whether or the desired protection is to prevent compromise or prevent destruction. If the goal is to prevent compromise of the asset, the response force must arrive in time to prevent the threat from reaching the asset. The above timelines needs to be created according to the protection required and may be shorter or longer depending on differences between compromise and destruction of protected assets.

## 2-3 ESTABLISH REQUIREMENTS

2-3.1 Establish the requirement for ESS early in the planning process.Establishing the requirement necessitates an interdisciplinary planning team to ensure all interests related to a project are considered appropriately and how security fits into the total project design. The specific membership of the planning team will be based on local considerations, but in general, the following functions should be represented: facility user, antiterrorism officer, operations officer, security, logistics, engineering, life safety, and others as required. The interdisciplinary planning team will use the process in UFC 4-020-01 to identify the design criteria, which includes the assets to be protected, the threats to those assets (the Design Basis Threat), and the levels of protection to be provided for the assets against the identified threats. In addition to the above listed criteria elements, the planning team may also identify user constraints such as appearance, operational considerations, manpower requirements or limitations, and sustaining costs. That design criteria will be the basis for establishing the requirements of the ESS and other elements of the overall security solution.

2-3.3 For existing facilities, the design criteria is used to perform a vulnerability assessment, the results of which are used to establish the requirements for the ESS. For new facilities, the design criteria is used to establish the requirements directly. The levels of protection will be the most important criteria element in establishing the ESS requirements. The process outlined in UFC 4-020-02 establishes the planning requirements. It also provides a risk management process that can be used to evaluate the resulting requirement. Figure 2-4 depicts the life cycle of an ESS.

**Figure 2-4. Project Process**

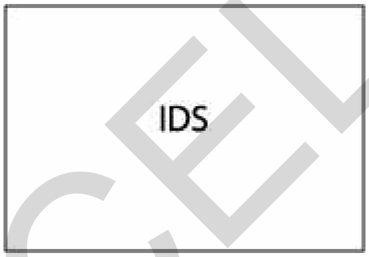

Assess/Identify Critical Asset
Establish Design Basis Threat
Establish Level of Protection
Assess Risk
Establish Planning Requirements
Planning Process
Security Engineering Facility Planning Manual
UFC 4-020-01
Validate Planning Requirements
Define Protective Measures
Assess Risk
Establish Design Requirements
Preliminary Design
Security Engineering Facility Design Manual
UFC 4-020-02
Design of ESS
Design
Scope of this Guide.
UFC 4-021-02
Construct
Test
Maintain

## 2-4 SYSTEM COMPLEXITY

2-4.1 **General.** ESS can range from simple to complex systems. While there may be some different views or definitions of what constitutes a simple or a complex system, this guide will use the criteria described in this section. The definitions used are an academic basis for presenting different system configurations and integration needs rather than standardized industry terminology, which does not exist for defining system complexity.

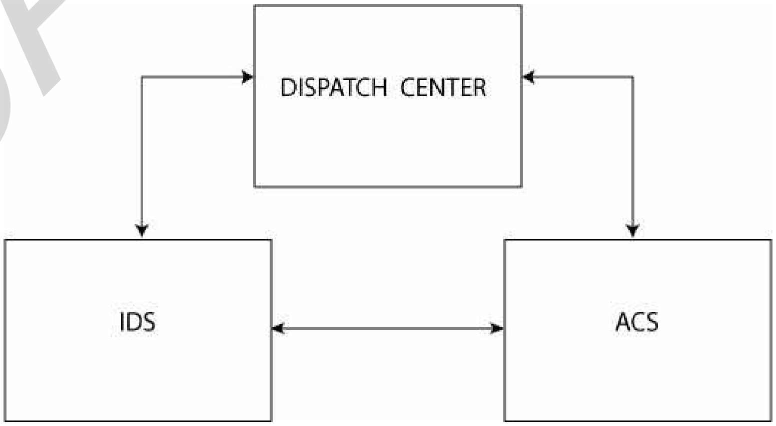
2-4.2 **Simple System.** The simplest ESS consists of a single ESS subsystem. For example, a simple IDS at a low value asset is a simple system as shown in Figure 2-5. Other examples are an IDS with door contact, motion sensors, break-glass sensors and other digital input type sensors that do not require integration with another ESS subsystem. Another example of a simple system would be a basic CCTV system of two cameras going to a Digital Video Recorder (DVR). Figure 2-5 shows a block diagram of a simple system.

**Figure 2-5. A Simple ESS System**



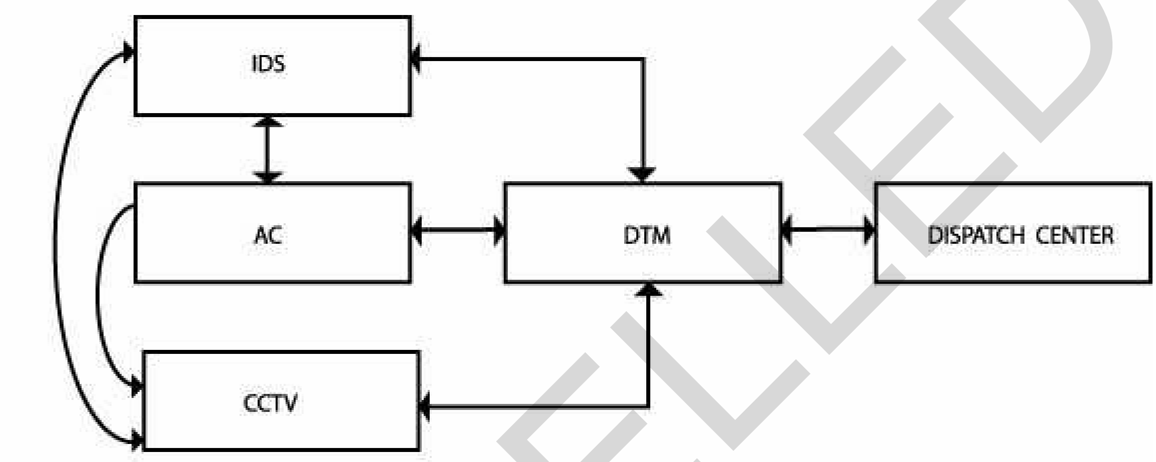
2.4.3 **Intermediate System**. An intermediate system contains elements of at least two ESS subsystems requiring integration. One example would be an ESS system requiring both an ACS and an IDS. A basic block diagram for this type of system reporting to a common Dispatch Center is shown in Figure 2-6.

**Figure 2-6. Intermediate System with Separate ACS and IDS**



2-4.3.1 **Combining ACS and IDS.** Virtually all ACS can accommodate digital input signals. Quite often it is possible to combine ACS and IDS when the IDS inputs are limited to simple digital input devices that do not require separate IDS controllers. Examples of these types of digital input IDS devices are door contacts, glass-break sensors, and motion sensors.2-4.4 Complex System. A complex system has a separate ACS and IDS system as well as a CCTV system communicating to a Dispatch Center through a DTM as shown in Figure 2-7.

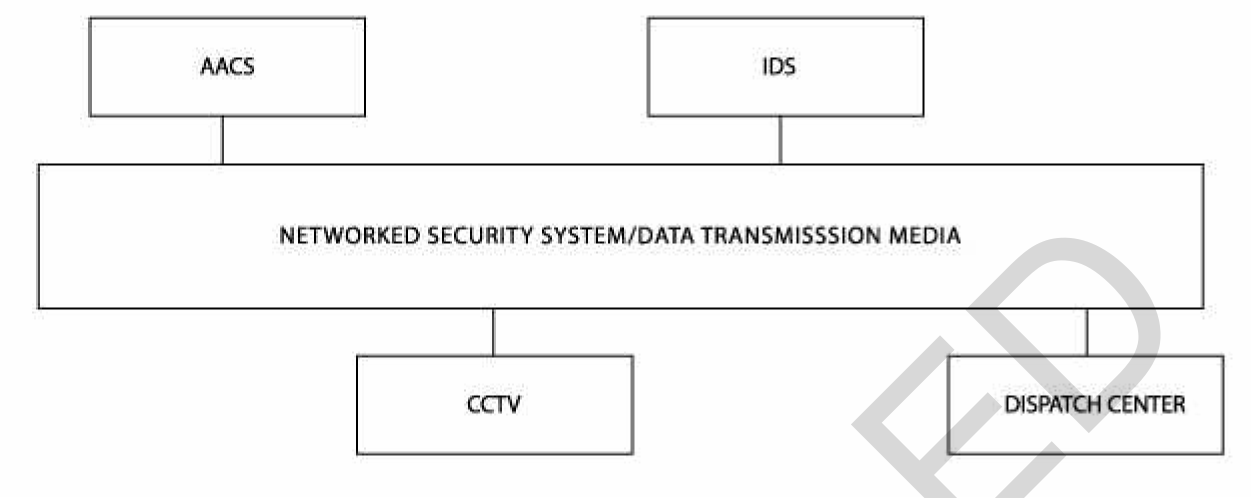
**Figure 2-7. Complex System With Separate ACS, IDS, and CCTV Subsystems**



In Figure 2-7, the curved line from the ACS/IDS to the CCTV system represents the interface that occurs between an alarm event (door contact alarm or fence detection alarm) to the action that causes the output from a CCTV to be displayed on an alarm indication screen and provide alarm annunciation in the Dispatch Center. The interface can vary from hardwired contacts to intelligent data communications. System interfaces and integration are described further in Chapter 8, "ESS Subsystem Integration."

2-4.5 **Networked System.** Figures 2-5, 2-6, and 2-7 show discrete systems. An emerging trend in the security industry is an evolution towards networked systems as shown conceptually in Figure 2-8.

**Figure 2-8. Networked System**



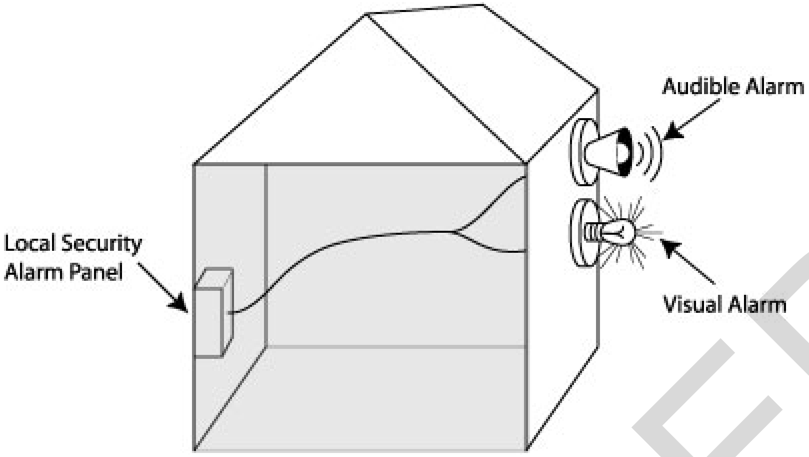
The networked security system operates on a single network with drivers to the different discrete components of the subsystems. While it is possible to procure networked systems, security suppliers are at different stages of development of providing networked systems for all ESS capabilities. At this writing, a lot of effort is being spent by individual vendors of ACS, CCTV, IDS and DTM to partner with other subsystem suppliers or write software drivers to achieve a networked ESS. Typically, networked security systems are typically a Proprietary Security Network. Refer to Chapter 8, “ESS Subsystem Integration” for more information.

## 2-5 MONITORING METHODS

2-5.1 **General.** Determine the alarm monitoring method early in the project planning process. There are several different monitoring methods. Monitoring configurations, as defined in DoD 0-2000.12-H, including local alarm, central station, connection, and proprietary station. It is vital that the ESS designer understand the need to identify the Dispatch Center and type of communications early in the project design.

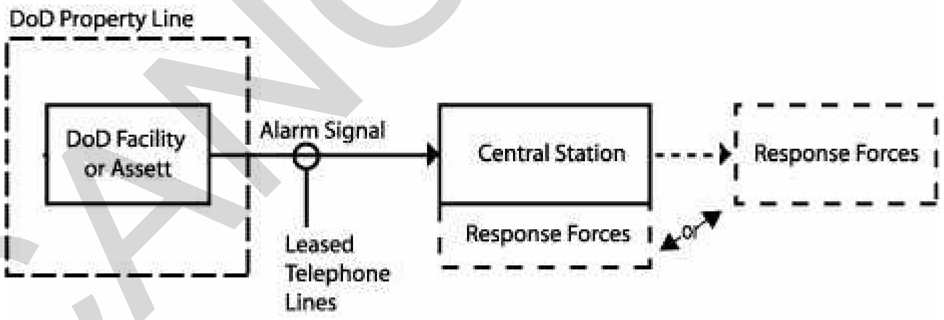
2-5.2 **Local Alarm**. Local alarms actuate a visible and/or audible signal, usually located on the exterior of the facility. Refer to Figure 2-9. Alarm transmission lines do not leave the facility. Response is generated from security forces located in the immediate area. Without security forces in the area, response may only be generated upon report from a person(s) passing through the area or during security checks. Local alarms may offer some deterrence value. Local alarm systems do not initiate the Detect, Delay, Respond sequence.

**Figure 2-9. Local Alarm Monitoring**



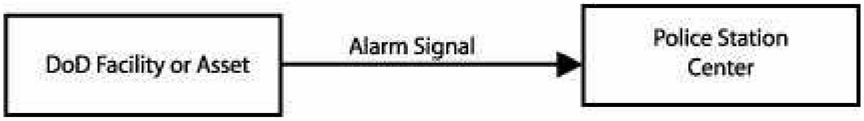
2-5.3 **Central Station.** Devices and circuits are automatically signaled to, recorded, maintained, and supervised from a central station owned and managed by a commercial firm with operators in attendance at all times. The Central Station personnel monitor the signals and provide the response force to any unauthorized entry into the protected area. Connection of alarm equipment to the central station is usually over leased telephone company lines for systems of significance. Dial-up modems maybe used for simpler systems. Refer to Figure 2-10.

**Figure 2-10. Central Station Monitoring**



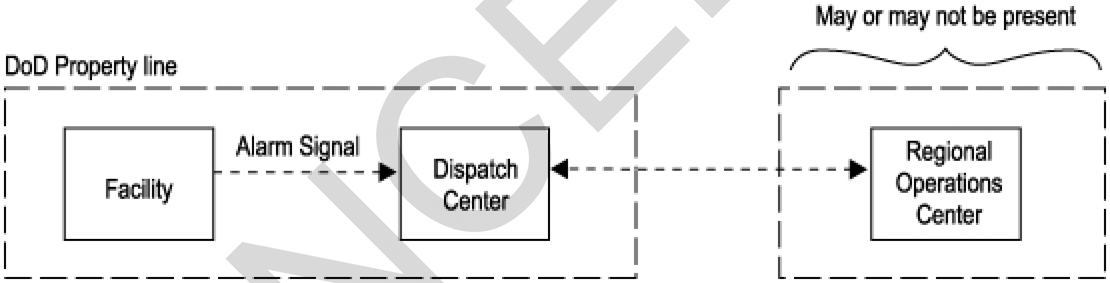
2-5.4 **Police Connection.** Police connection systems are transmitted to and annunciated at a local police agency dispatch center that records alarm annunciation. Connection to the police is primarily over leased telephone lines. Police personnel respond to alarms. A formal agreement with the police department is required to ensure monitoring and response requirements. Often police departments impose a penalty after some quota of false alarms, thus the sensitivity is often turned down to minimize nuisance alarms and may result in missed indications. Police responders may be attending to other emergencies and unavailable to respond when needed. Police connection configurations are typically used for facilities, which are not located on a DoD base or installation. Examples of facilities, which might be protected by a police connection configuration, include medical clinics, base exchanges, commissaries, and Reserve Centers. Refer to Figure 2-11 for a diagram of a police station connection.

**Figure 2-11. Police Connection Monitoring**



2-5.5 **Proprietary Station.** This system is similar to a central station operation, except that ESS monitoring or recording equipment for all ESS at the installation is located within a constantly-staffed Dispatch Center on an owner's property. Proprietary stations are prominent throughout DoD installations where Dispatch Centers are owned, maintained, and staffed by DoD personnel, who comprise the response force. The installation security force responds to all ESS alarms. As a basic configuration, the Dispatch Center may be centrally located at an installation. Two possible configurations of a Proprietary Station Dispatch Center are shown in Figure 2-12: a Dispatch Center centrally located at a base and an alternative configuration is a detached Regional Dispatch Center (RDC).

**Figure 2-12. Proprietary Station Monitoring**



2-5.6 **Summary.** Table 2-3 provides a summary of the pros and cons of each type of monitoring station method.

**Table 2-3 Pros and Cons of Monitoring Methods**

| | **Pros** | **Cons** |
|---|---|---|
| **Local Alarm Station** | Easy to implement<br>Cost effective<br>Simple | No guaranteed response, relies on support forces being in audible/visual range |
| **Centralized Station** | Does not require any additional space or building<br>Probably does not require any additional staffing | Requires an existing Central Station<br>Some complexity in establishing connection<br>May rely on non-DoD forces<br>CCTV capability may be limited or non-existent |

| | | |
|---|---|---|
| **Police Connection** | Direct communication with law enforcement/response forces without delay. | Requires a cooperating law enforcement station with space and equipment.<br>Must consider separate archiving resource<br>Probably does not have CCTV assessment capability.<br>Ongoing fee may be required for monitoring<br>Interface connection is required.<br>Systems often operate with reduced sensitivity to minimize the number of nuisance alarms. |
| **Proprietary Station** | Not reliant on outside sources.<br>Should have CCTV assessment capability.<br>May have Motion Path Analysis (IDS) capability. | Requires 24/7 trained personnel; possibly increased staffing.<br>Requires real estate space and fit-out hardware.<br>Increased recurring labor cost of Dispatch Center operators. |

# CHAPTER 3

# ACCESS CONTROL SYSTEMS

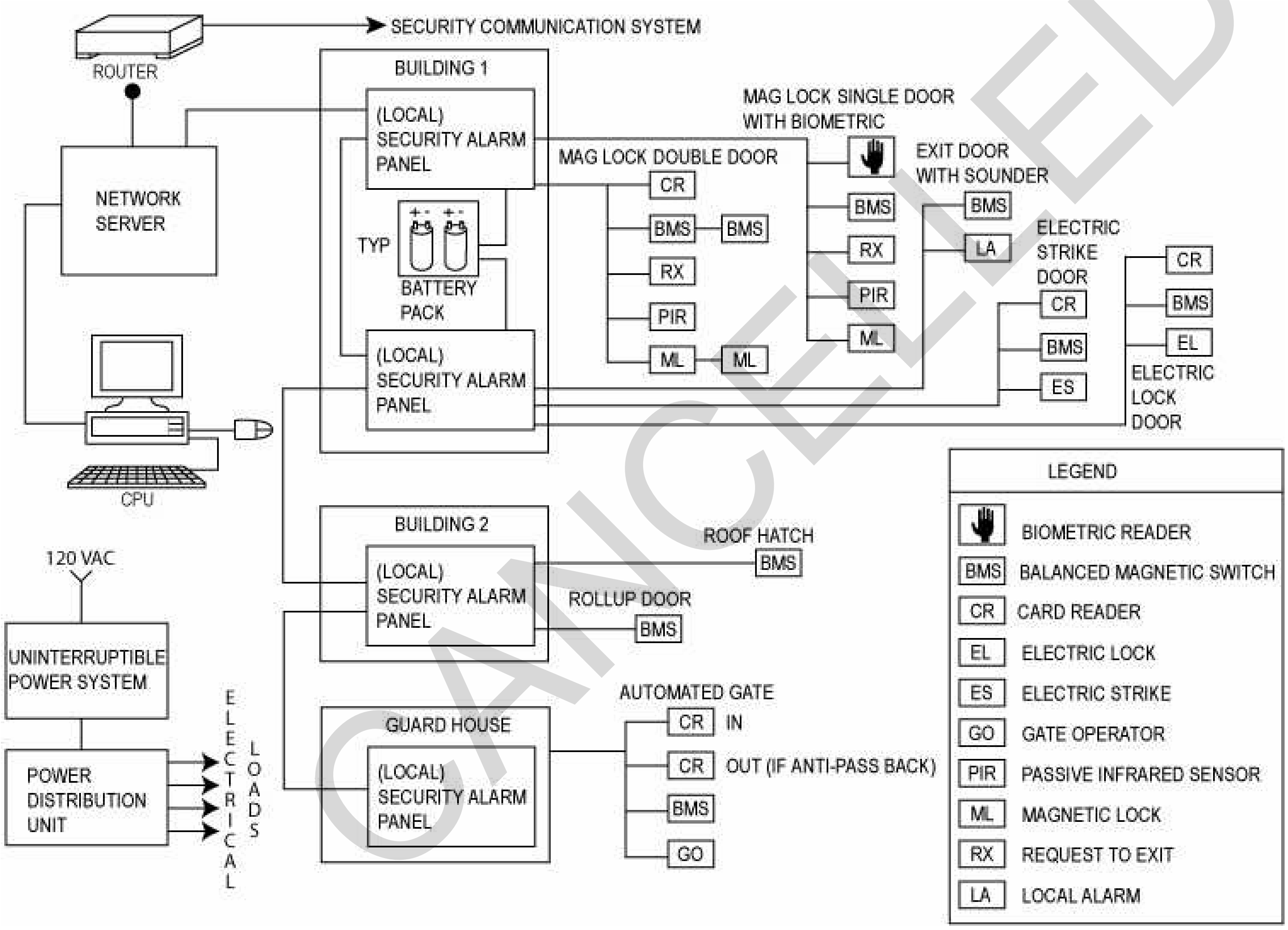
## 3-1 OVERVIEW

3-1.1 The function of an ACS is to ensure that only authorized personnel are permitted ingress and egress from a controlled area. The ACS should be able to log and archive all transactions and alert authorities of unauthorized entry attempts. ACS can be interfaced with the CCTV system to assist security personnel in the assessment of unauthorized entry attempts.

3-1.2 As illustrated in Figure 3-1, an ACS has many elements, including electric locks, card readers, biometric readers (when required, but not always part of every system), alarms, and computer systems to monitor and control the ACS. An ACS generally includes some form of enrollment station used to assign and activate an access control device. Detailed descriptions of the various elements of an ACS are described later in this chapter.

3-1.3 In general, an ACS compares an individual's credential against a verified database. If authenticated, the ACS sends output signals which allow authorized personnel to pass through controlled portals such as gates or doors. The system has the capability of logging entry attempts (authorized and unauthorized) that are archived. (Event and tracking logs are discussed in more detail in a subsequent subsection.) Typically the ACS interfaces with the IDS for input of digital alarm signals at access portals controlled by the ACS. An example of this would be "door forced" alarms at a card reader controlled door. Similarly, the ACS interfaces with the CCTV system in that cameras could be placed at remote gates to verify identity of entrants before manually actuating the remote gate. Signals from the ACS are communicated to the Dispatch Center through the transmission lines of the DTM. Further information on the specifics of ACS interfaces with the rest of the ESS are developed in Chapter 8, "ESS Subsystem Integration."

**Figure 3-1. Example Access Control System (ACS)**



## 3-2 ACS ENTRY-AUTHORIZATION IDENTIFIERS

3-2.1 ACS entry-authorization identifiers are grouped into three categories:

- Credential devices
- Coded devices
- Biometric devices

These devices operate on three basic techniques:

- Something a person has, such as a common access card (CAC), swipe card, or proximity card
- Something a person knows, such as a personal identification number (PIN)
- Something a person is or does, such as a biometric identifier

3-2.2 **Credential devices**. Credential devices identify a person as having legitimate authority to enter a controlled area. A coded credential (such as a plastic card or key) contains a prerecorded, machine-readable code. When the card or key is read, an electric signal unlocks the door if the prerecorded code matches the code stored in the system. A credential device only authenticates the credential; it assumes a user with an acceptable credential is authorized to enter. Various technologies are used to store the code within a card or key. The most common types of cards are described in more detail in the section *Card Types*.

3-2.2.1 Advantages and disadvantages of using credential devices are shown in Figure 3-2.

**Figure 3-2. Advantages and Disadvantages of Using Credential Devices**

**Advantages**

- Cards and card readers are reliable.

**Disadvantages**

- Cards can be lost or stolen.
- Some types of cards can easily be duplicated.

Each type of card and card reader has its own advantages and disadvantages. Refer to the subsections *Card Readers* and *Card Types* in the section *ACS Equipment* in this chapter for more on the advantages and disadvantages of each.

3-2.3 **Coded devices**. Coded devices such as a keypad or microprocessors operate on the principle that a person has been issued a code or PIN to enter into the device that will verify the authenticity of the code entered. Any person entering a correct code is authorized to enter the controlled area.

3-2.3.1 Advantages and disadvantages of using coded devices are shown in Figure 3-3. For information about the different types of coded devices see the section *Keypads and PIN Codes,* later in this chapter.

**Figure 3-3. Advantages and Disadvantages of Using Coded Devices**

Advantages

- Keypads are compact and easily understood.
- Different codes may be used to give access to different points and doors.
- Maintenance is easy.
- Keypads are not expensive. They are reliable and easily replaced or repaired. Little complex hardware is needed.
- No cards or tokens need be carried so there is nothing to lose.
- A duress code, known only to the user, can be input covertly if a legitimate person is forced to enter under duress.

**Disadvantages**

- Codes are easily passed on to other unintended or unwelcome visitors.
- The code can possibly be viewed by others and thus used for unapproved entry.
- Hands-free operation is not an option.
- The number of allowable unique codes can be limited. For example, a four-digit PIN only provides 10,000 different possible codes.

3-2.4 **Biometric devices**. Biometric devices rely on measurements of biological characteristics of an individual, such as a fingerprint, hand geometry, handwriting, voice, or iris patterns. Selected individual characteristics are stored in a device's memory or on a card, from which stored reference data can be analyzed and compared with the presented template.

3-2.4.1 A one-to-many or a one-to-one comparison of the presented template with the stored template can be made, and access granted if a match is found (depending on the authorized security level). There are two important acceptance results of which to be aware. They are *false reject* and *false accept*. False reject is denying entry to authorized personnel. This is inconvenient, but does not compromise security. False accept is granting access to non-authorized personnel. This is the most critical result, as highly-secure facilities cannot afford the error of a false accept. All ACS have some percentage of false positive (accept) alarm signals, ESS system designers should understand the issues and work to minimize the number of false positive (accept) events.  From a logistics perspective, missions cannot be accomplished if false reject rates are high and authorized personnel are regularly unable to enter their workspace or facility.

3-2.4.2 Advantages and disadvantages of using biometric devices to grant or deny access are shown in Figure 3-4. For information about the different types of biometric technologies, see the subsection *Biometric Readers* in the section *ACS Equipment* in this chapter.

**Figure 3-4. Advantages and Disadvantages of Using Biometric Devices**

Advantages

- They provide automated verification that the person attempting to gain access is authentic.
- Biometric credentials are extremely difficult to duplicate.

**Disadvantages**

- The cost is slightly higher.
- Longer verification time.
- Require special housings.
- Do not work well in exterior environments

3-2.5 **Combining credentials**. A site's security can be significantly enhanced by combining two or more types of automated access control credentials - such as a biometric characteristic with a smart card or a proximity card with a PIN code. However, combining credentials results in increased verification time and will decrease throughput rate. Throughput time should be considered when making decisions about whether or not to use redundant verification. Another consideration in combining two types of credentials is that a system can be required to use one device during lower risk times (such as during normally staffed times) and two devices can be required for entry after hours. The same philosophy can be applied for access control enhancement during times of heightened force protection threat levels. A risk assessment needs to be performed to help determine the degree or level of credentially.

3-2.6 **Identification Method Selection**. The type of identification method (card, PIN, biometric attribute or a combination thereof) that will be used needs to be determined early in the project. Identification of the existing ACS token media and system capacity should be assessed during project kickoff or the early programming phase. Per DoD Directive 8190.3, the CAC is the preferred card.

## 3-3 OTHER ACS IMPLEMENTATION CONSIDERATIONS

3-3.1 Other things to consider implementing as part of an ACS include anti-passback, anti-tailgating, the two-man rule, and performing event tracking. These are described in the following sections.

3-3.2 **Life Safety Code Compliance.** Anti-tailgating and anti-passback features must be consistent with the philosophy of the Life Safety Code and the Means of Egress for Buildings and Structures, unless specifically over-ruled by Government Authority.

3-3.3 **Anti-passback**. Anti-passback is a strategy where a person must present a credential to enter an area or facility, and then again use the credential to “badge out.” This makes it possible to know how long a person is in an area, and to know who is in the area at any given time. This requirement also has the advantage of instant personnel accountability during an emergency or hazardous event. Anti-passback programming prevents users from giving their cards or PINs to someone else to gain access to the restricted area. In a rigid anti-passback configuration, a credential is used to enter an area and that same credential must be used to exit. If a credential holder fails to properly “badge-out”, entrance into the secured area can be denied. Anti-passback is a standard feature for Commercial-Off-The-Shelf (COTS) access control systems and is typically disabled but can be enabled through software programming.

3-3.3.1 An alternative approach to “badging out,” which is not as rigid as the process described above, is use of a time delay on entrance readers. In this design, the credential (Card or PIN) can not be reused within a prescribed minimum time period. This time delay feature can be programmed and set for a time period such as a half-hour. During the half-hour time period, the same card or PIN can not be used for a second entry. While affording some increased security, this process is not as rigid or secure as a ‘badge-out” process.

3-3.4 **Anti-tailgating**. While not commonly required, a project security requirement may be to deter tailgating. Tailgating is the act of a person following another authorized person closely in order to gain ingress through the same portal when the authorized person’s credential grants access. An example of a simple anti-tailgating requirement would be a pedestrian turnstile for access control. Since turnstiles are easily defeated, when significant, anti-tailgating measures are required, high-security vestibules or guard-controlled entrances can be a solution. Such application may slow down access.

3-3.5 **Two-man Rule**. The two-man rule is a strategy where two people must be in an area together, making it impossible for a person to be in the area alone. Two-man rule programming is optional with many identification systems. It prevents an individual cardholder from entering a selected empty security area unless accompanied by at least one other person. Once two token holders are logged into the area, other token holders can come and go individually as long as at least two people are in the area. Conversely, when exiting, the last two occupants of the security area must leave together using their tokens. Use of the two-man rule can help eliminate insider threats to critical areas by requiring at least two individuals to be present at any time. Most ACS software will enable the assignment of a *specific* second person that can be established (such as clearance escort requirement).

3-3.6 **Exit Technologies**. While access control is principally concerned with entry requirements, some consideration must be given to exit technologies and methods. Door hardware or locking mechanisms specified to enter access portals influence exit hardware. Life safety codes in the United States dictate that personnel can not be locked in such that they are restricted from free exit. When an opening is locked from the public side and free exit is required from the secure side, there are several methods that can be employed as discussed below. Refer to Chapter 9 for more information.

3-3.6.1 The simplest door hardware is a “crash bar”. This strictly mechanical device merely requires exiting personnel to hit the “push-to-unlock” bar. If an electric strike is used as a door lock, generally the door has a twist door-knob handle that allows free exit.

3-3.6.2 If magnetic locks are used to secure the door than both an automatic and manual method of existing the door must be provided. Generally, the manual method is a Request to Exit button, sometimes abbreviated as a REX. When this device is pressed, power to the door locks is shunting allowing exit. The most common form of an automatic sensing device that will release the door lock when a person approaches a door in the exiting direction is a Passive Infrared Sensor (PIR). This device senses the infrared heat signature of a person and automatically shunts door lock power allowing free exit. PIRs have a significant security shortfall in that any person passing by or loitering in the sensing area of a the opening can activate the PIR and shunt door lock power. For this reason, magnetic locks should be the designer’s last choice for door locking mechanisms.

3-3.6.3 Card readers or keypads can be used for anti-passback, “badge out” procedures but require building code variance or approved special circumstances for locking an exit portal for a normal existing individual. Badge out card readers over more specific identification of existing personnel over keypads, where a number of individuals could have knowledge of the exit numerical code.

**Table 3-1 Exit Technologies (Pros and Cons)**

| | **Pros** | **Cons** |
|---|---|---|
| **Door Hardware** | Easy to implement<br>Cost effective<br>Simple | Does not “track” who left the facility or space.<br>No additional security. |
| **Request-to-Exit Button** | Slightly simpler to implement than keypads or cardreaders.<br>No additional Pros, typically mandated in U.S. by use of “mag locks” as door locking device. | Generally requires complementary automatic exiting devices such as a PIR.<br>No additional security.<br>PIRs can release the door lock if someone lingers in detection cone. |
| **Keypads** | Some additional security afforded in that exiting person needs to know the exit code. | Requires variance or alternate method to U.S. life safety code for exit doors.<br>Exit code can be shared.<br>Additional construction cost. |

| | | |
|---|---|---|
| **Cardreaders** | Can be used to achieve anti-passback function.<br>Allows tracking of exiting personnel by individual identification. | Requires variance or alternate method to U.S. life safety code for exit doors.<br>Extra construction cost and programming. |

3-3.7 **Event tracking/event logs**. Event tracking/event logs are lists or logs of security events recorded by the access control system that indicate the actions performed and monitored by the system. Each event log entry contains the time, date, and any other information specific to the event.

## 3-4 ACS EQUIPMENT

3-4.1 Once the type of identifier and other implementation strategies are determined, the type of equipment to use can be determined. Various types of ACS equipment are available, as described in the following sections.

3-4.2 **Badging Equipment**. When credentials have associated identification badges, ancillary badging equipment is needed. Note that besides the CAC issued to all government employees, supplemental badging may be required during CAC card implementation-transition or for certain restricted access facilities. The Activity must provide justification to support the requirement for any badging equipment. This equipment should be scrutinized before deciding to purchase. Badging equipment includes:

3-4.2.1 Camera for capturing photographs

3-4.2.2 Software for creating badge images

3-4.2.3 Signature capture tablet

3-4.2.4 Biometric template capture device (where applicable)

3-4.2.5 Badge printer capable of printing a color ID template on the front and back of the badge, and capable of encoding a magnetic stripe or smart card (where applicable). There are new technology printers that are capable of printing pseudo holograms on the clear protective laminate, which may be considered for higher security applications.

3-4.2.6 Computer for retention and programming of the security credential database. This computer may be a stand-alone or client workstation that is connected to the ACS server database in a client/server architecture.

3-4.2.7 Equipment to encode badges (depending on types of badges). The badge printer may be equipped with a magnetic stripe encoder or a separate stand-alone magnetic stripe encoder or both may be necessary where required. The new GSC-IS V2.1 contactless technology tokens require a card reader/writer to encode (not encrypt) the token. For more information, refer to the *Government Smart Card Interoperability Specification.*

3-4.2.8 If there is no existing badging location and equipment, the design must include the badging infrastructure described above as well as space allocation for equipment and storage requirements.

3-4.2.9 Badging may require an interface to an existing personnel database where the necessary information is stored and maintained. If so, requirements for this database interface and security must be established

3-4.3 **ACS Central Processing Unit (CPU)**. The CPU is the physical intelligent controller(s) where the ACS application software and database reside and where all ACS system activity is monitored, recorded into history, commanded and controlled by the operator. Examples of ESS CPU's include: microprocessors, servers, programmable logic controllers (PLCs), or even personal computers (PCs). Conceptually, the CPU can be thought of as the "brain" of the ACS system. Formerly, the CPU was a discrete component located at the "head-end" of the system, typically the Dispatch Center. Current state-of-the-art ACS use distributed intelligence that allows each local security panel to hold (in microprocessor memory) the system logic for its associated devices. The CPU retains the system specific programming for "action/reaction" logic steps necessary for an ACS to allow entry (access) for authorized personnel and deny access to unauthorized personnel. A sample sequence is shown in Figure 3-5.

3-4.3.1 Communications failure between the CPU and the local access control processor equipment could result in new users not being permitted entry. Additionally, during any communication failure, users who are no longer authorized will still be able to enter the area. It is important to provide sufficient backup power capability for the CPU, local processors, and other critical infrastructure to prevent the loss of control of authorized access. Redundant, fault-tolerant communication systems are required in high-security areas where loss of communications (including partial links) cannot be tolerated.

3-4.3.2 A specialized case of a CPU is a Premises Control Unit (PCU). A PCU is a DCID 6/9 term used to describe a specific controller located within the confines of a Sensitive Compartmented Information Facility (SCIF). Per the *Physical Security for SCIFs:* "A PCU is a device that receives changes of alarm status from IDS sensors, and transmits an alarm condition to the monitoring station." The PCU resides in an internal location, safe from external tampering and controls and monitors ESS equipment for the protected area as shown in Figure 3-6.

**Figure 3-5. Basic Access Control Sequence**

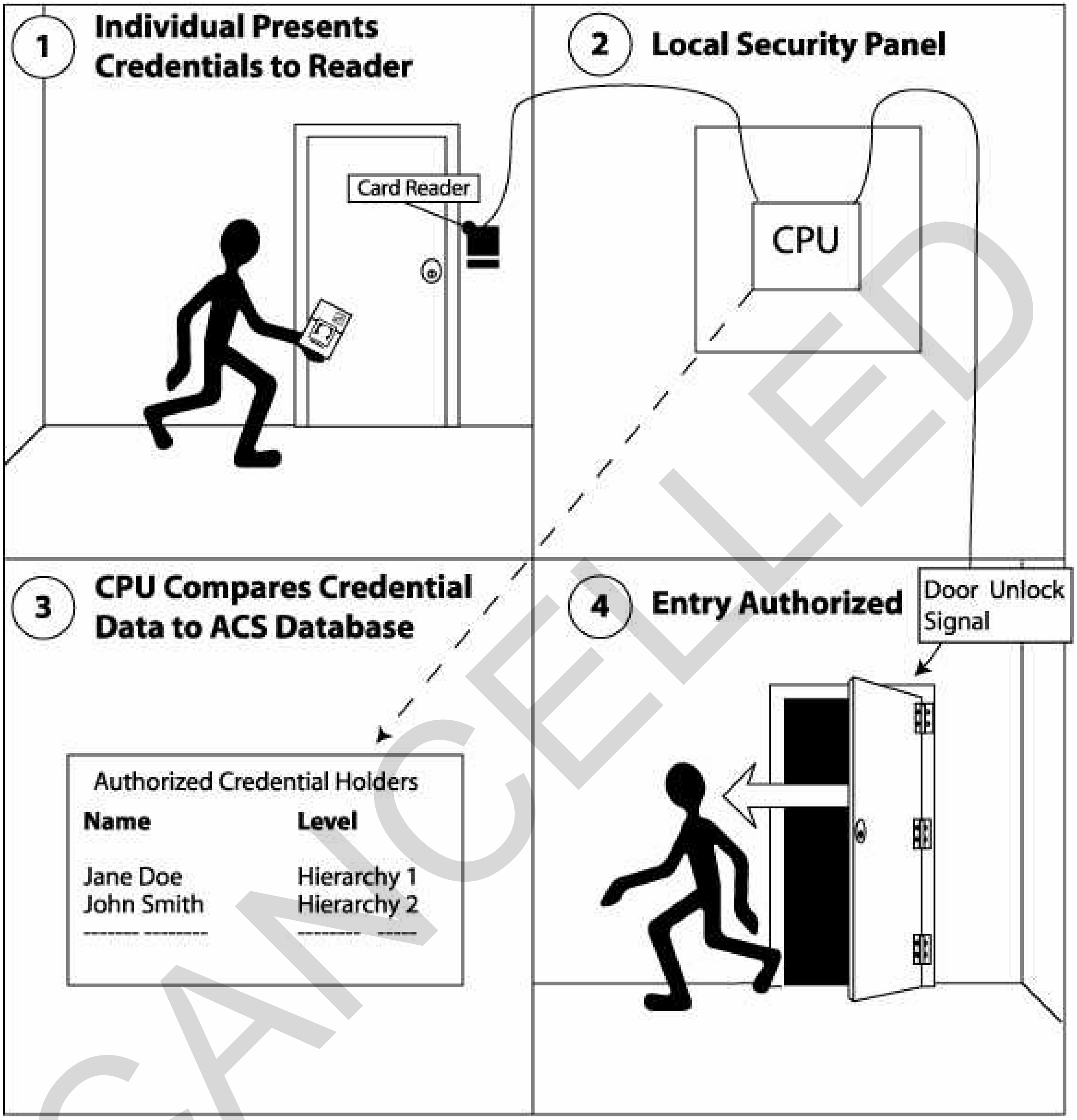
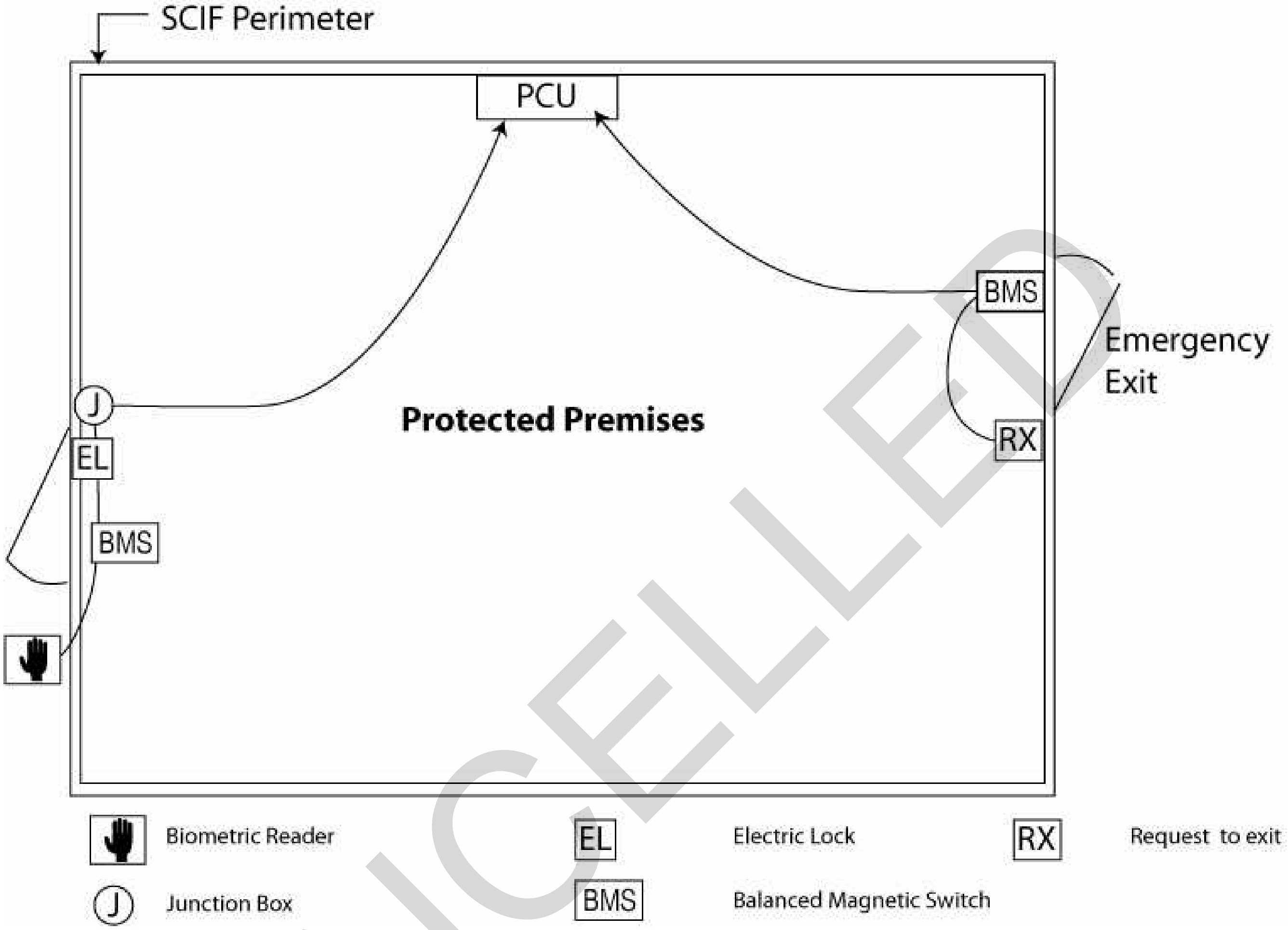


**Figure 3-6. PCU In A SCIF**



3-4.4 **System Display**. The system display is the screen or monitor that allows personnel to view and interact with the ACS hardware and software. Typically, it is a computer screen. The location of the system display should be identified early in the design process. The system display and control can be anywhere a computing device is connected to the network. The software can reside on any computing device (preferably a server) and be accessed by anyone connected to the network provided they have access rights to the software. Furthermore, it can be made accessible to the Dispatch Center. This means that existing computer systems can be used when integrating the system. Contact the base security and communication office (information technology) for system capacity issues and coordination.

3-4.5 **Security Alarm Panels**. Security alarm panels collect inputs from card readers, biometric devices, door sensors, and so on. and provide output signals to electronic door locks, electric strikes, or gate operators. Security alarm panels are connected to the CPU that provides the database intelligence for determining whether to grant or deny access. Newer security alarm panels incorporate the following features:

3-4.5.1 Multiple connection methods such as dial-up modem, serial (RS-232), multi-drop (RS-485), and network TCP/IP.

3-4.5.2 Integrated CCTV camera connectivity, allowing CCTV camera information to be shared with the ACS.

3-4.5.3 Capability for asset tracking within a facility, such as with radio frequency identification (RFID) tags connected to critical assets.

3-4.5.4 Capability for incorporating duress or panic alarm capability.

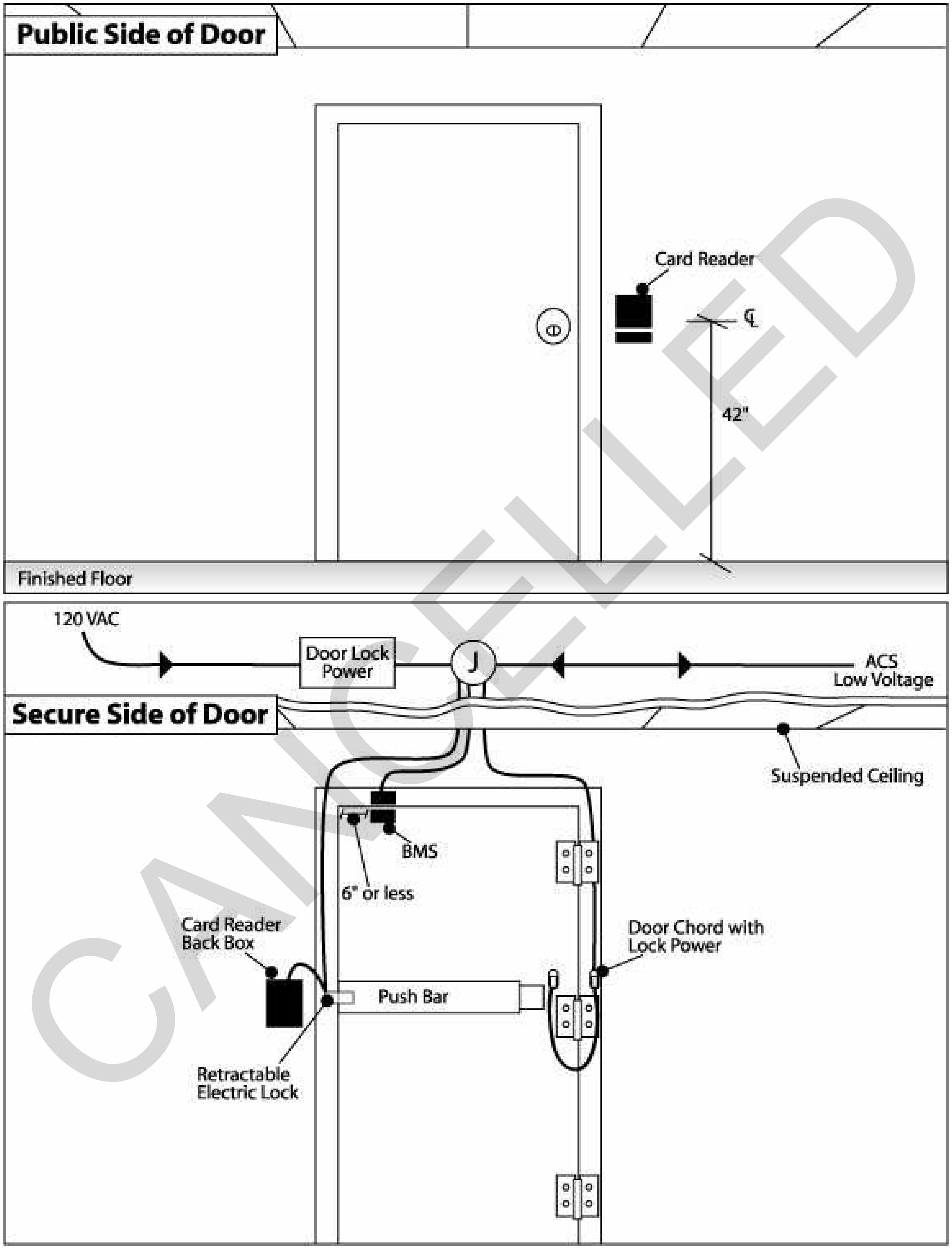
3-4.6 **Card Readers**. The most common form of credential verification is a security card reader.

3-4.6.1 **Types of Card Readers.** There are a number of different types of card readers**.** Insertion readers require that you insert the card into a slot that is just large enough to accommodate the card and then remove it. Swipe readers require that you swipe the card through a long narrow slot that is open at each end. Proximity and contactless readers require that you hold the card in front of the blank face of the reader.

3-4.6.2 Insertion and swipe readers, while functional, are older technologies; however, at this writing the use of the CAC requires use of the insertion type magnetic stripe reader or a bar code reader. Insertion or swipe readers require the credential to be inserted into the reader and the card can wear out over time. Once the CAC is converted to a contactless read capability, use of insertion or swipe readers should be an unusual design for new projects because of the dated technology. Until the CAC is converted to contactless read capability, the insertion magnetic stripe reader is preferred over the bar code reader, which is more easily compromised. Proximity readers are popular and require the user to pass the card within an adjustable distance (one to two inches from the reader). While commonly used in commercial non-DoD applications, testing has demonstrated that it is possible to intercept the unencrypted (125kHz proximity card) signals. Smart cards are also wireless, contactless credentials that can be read in close proximity to a smart card reader.

3-4.6.3 Figure 3-7 displays a typical configuration for a single door equipped with a card reader and electric lock. Refer to the subsections on *Doors* and *Door Locks* in Chapter Nine, General Requirements and Cross-Discipline Requirements for additional information on door hardware types and interface considerations.

**Figure 3-7. Sample Card Reader Door Configuration**



3-4.7 **Card Types**. Card readers use a number of different card types, the most common in use are described in the following subsections.

3-4.7.1 **Magnetic Stripe Cards**. Magnetic stripe (mag stripe) cards consist of a magnetically-sensitive oxide strip fused onto the surface of a PVC material. They are inexpensive, easily manufactured, and can carry alphanumeric data. (Magnetic cards used within the DoD should comply with SEIWG-012, which specifies numeric data only.) A magnetic stripe card is read by swiping it through a reader or by inserting it into a position in a slot. A magnetic stripe card can be individualized by color coding the cards and printing photo information onto them. The magnetic stripe card is disadvantaged in that it may be physically damaged by misuse and its data can be affected by magnetic fields, even when they are of only low potential. Other problems associated with this type of card are related to the high volume of equipment available for the reading and copying of cards so that unauthorized duplication and copying can never be entirely negated.

3-4.7.2 **Proximity Cards**. Proximity cards (prox cards) use embedded antenna wires connected to a chip within the card. The chip is encoded with the unique card identification. Currently, the standard proximity card operates at a frequency of 125kHz. Distances at which proximity cards can be read vary by manufacturer and installation. Readers can require the card to be placed within a fraction of an inch from the reader to six inches away. Having the card out and at the same height of the reader, background electrical interference levels, and sensitivity of the reader affect the distance at which a card can be read. Proximity card technology (125kHz) should not be confused with wireless, contactless (13.56MHz) technology.

3-4.7.3 **Wiegand Cards.** The following information is cited from *Effective Physical Security (page 196):*

> The Wiegand card is also called an embedded-wire card. The technology is based on the Wiegand Effect, a phenomenon observed when specifically prepared ferromagnetic wires suddenly reveres themselves on exposure to an external magnetic field. Wires inside the Wiegand card are formed in a permanently tensioned helical twist. The order and spacing of the wires establish a unique code for each card. The magnetic reversals in the wires are converted into distinct, consistent electrical pulses that are read and processed. The card's thickness and stock composition make it resistant to pocket damage; however, it is susceptible to malfunction arising from wear after many passes through reader slots. The card is moderately priced, but capable of storing a moderate amount of data.

3-4.7.4 **Smart Cards**. Smart cards are credential cards with a microchip embedded in them. The term "smart card" can define cards that simply carry data, but more commonly is used describe cards with integral microprocessing and read/write data storage capability. Smart cards are available as a "Contact" type or more commonly as a "Contactless" (and wireless) type. An example of a "Contact" smart card is one which can interface to a computer through the embedded contact. The contactless, wireless smart card operates at 13.56 MHz, which is more than a hundred times faster than the data exchange rate of 125kHz proximity cards. There are also hybrid cards available, which have either both types of smart card chips in one plastic body or have both contact and contactless interfaces to one microprocessor in the plastic body. Smart cards can store enormous amounts of data such as access transactions, licenses held by individuals, qualifications, safety training, security access levels, and biometric templates. One principal security advantage of smart cards is that cryptographic capabilities can be used to send card information to legitimate readers and encrypts that transmission such that the system remains immune from replay attacks. It is difficult to copy security credential information onto a forged card. For more information on the federal standard for electronic smart cards, refer to NIST FIPS 201.

3-4.7.5 **Common Access Card (CAC)**. The CAC is a credential used by the DoD to allow access to DoD computers and physical locations worldwide. For each individual, one card works for all access to computers and physical locations. The CAC is a JAVA-based smart card. It can store a number of personal demographic data elements. It supports multiple bar codes and a magnetic stripe for legacy applications, making the card extremely versatile. A standard developed by the Security Equipment Integration Working Group, SEIWG-012, provides details on the formatting of the information to be encoded on track two (2) of the magnetic stripe of the CAC. SEIWG's intent is to ensure that cards can store enough data to determine information such as the individual cardholder, the branch of the military from which the card was issued, and the base from which the card was issued.

Per DoD Directive 8190.3, the CAC should be "the principal card enabling physical access to buildings, facilities, installations, and controlled spaces. This policy does not require DoD components to dismantle immediately current access systems, or preclude the continued use of supplemental badging systems that are considered necessary to provide an additional level of security not presently afforded by the CAC (e.g., such as entrance into a SCIF or other high security space). The DoD plan is to migrate to the CAC for general access control using the CAC's present or future access control capabilities. In the future, CACs will be contactless (13.56 MHz) compliant with ISO 14443 and NIST 6887 (Government Smart Card Interoperability Specification). This technology is proposed to be included in the next generation of CAC. For more information on the Government smart card program, refer to Http://smartcard.nist.gov/.

Since the CAC is not fully implemented, an additional badge may be required for dependants, contractors, temporary employees, host-nation workers or when an additional card provides an added capability not currently provided by the CAC.

3-4.7.6 **Operational Strategies.** Operational strategies for badge policy such as where the badge is worn, the type of photograph (if required), backgrounds for area authorization, rules of challenge, penalties for not wearing, and losing are important but are not within the scope of this design guide.

3-4.7.7 **Card Reader/Card Type Recommendation**. New projects should consider new technology smart cards and the CAC. Magnetic stripe readers used with the CAC allow the use of the encoding format defined in the SEIWG-012 standard (described in the previous section *Magnetic Stripe Cards*).

3-4.8 **Keypads and PIN Codes**. Coded devices use a series of assigned numbers commonly referred to as a PIN. This series of numbers is entered into a keypad and is matched to the numbers stored in the ACS. By itself, this technology does not offer a high level of security since a PIN can be stolen by even casual observation. However, coded devices can be effective when used in combination with another credential reading technology. Coded devices include electronic keypads and microprocessor-controlled keypads.

3-4.9 **Biometric Readers**. Biometric readers verify personal biological metrics (biometrics) of an individual. Biometric readers may be used in addition to credential devices or with a PIN code.

3-4.9.1 Biometric devices have uses at access control points, but may not be mature enough to use in throughput-critical applications such as vehicle entry gates. Designers have to evaluate the tradeoff between added security and decreased throughput.

3-4.9.2 Biometric readers are the future trend of security systems. Current gains in large-scale production of some types of biometric readers have brought biometrics close in cost to conventional card readers. Although biometrics are not as fast as other readers, these technologies are still evolving.

3-4.9.3 There are several types of biometric characteristics that can be used. The most common are described in the following sections.

3-4.9.3.1 **Fingerprint**. Fingerprint technology scans the loops, whorls, and other characteristics of a fingerprint and compares it with stored templates. When a match is found, access is granted (depending on the authorized security level). Advantages of fingerprint technology are that it is easily understood. Disadvantages are that the systems can be disrupted if cuts or sores appear on fingers or if grease or other medium contaminates the fingers and the scanning plates. Some systems create two templates for two different fingers, in the event that one finger is altered by injury or other means. Fingerprint technology is not convenient in environments where workers wear gloves. Early fingerprint readers were compromised by picking up a valid fingerprint from a reader with a manufactured “finger”. To combat this shortcoming of the technology, sensors were equipped with the ability to sense a pulse and temperature. Fingerprint technology is the first choice biometric method per the emerging FIPS201.

3-4.9.3.2 **Facial Image.** This technology measures the geometric properties of the subject’s face relative to an archived image. Specifically, the center’s of the subject’s eyes must be located and placed at precise (within several pixels) locations. Facial imaging is the backup technology for biometric authentication per FIPS 201.

3-4.9.3.3 **Hand Geometry**. This technology assesses the hand’s geometry: height, width, and distance between knuckle joints and finger length. Advantages of hand geometry are that the systems are durable and easily understood. The speed of hand recognition tends to be more rapid than fingerprint recognition. Hand recognition is reasonably accurate since the shape of all hands is unique. A disadvantage is that they tend to give higher false accept rates than fingerprint recognition. As with fingerprint technology, hand geometry is not convenient in environments where workers wear gloves.

3-4.9.3.4 **Handwriting**. Handwriting recognition analyzes the pressure and form of a signature. This technology is only used in an ACS without heavy traffic because the procedure of verification is slow. A PIN is typically entered into the system first so that the computer can more quickly find a template against which to identify the person seeking entry. Handwriting systems are not widely used.

3-4.9.3.5 **Voice Recognition**. Voice recognition identifies the voice characteristics of a given phrase to that of one held in a template. Voice recognition is generally not performed as one function, and is typically part of a system where a valid PIN must be entered before the voice analyzer is activated. An advantage of voice recognition is that the technology is less expensive than other biometric technologies. Additionally, it can be operated hands-free. A disadvantage is that the voice synthesizer must be placed in an area where the voice is not disturbed by background sounds. Often a booth has to be installed to house the sensor in order to provide the system an acceptable quiet background. Voice recognition systems are not widely used.

3-4.9.3.6 **Iris Patterns**. Iris recognition technology scans the surface of the eye and compares the iris pattern with stored iris templates. Iris scanning is the most accurate and secure biometric. After DNA, irises are the most individualized feature of the human body. Even identical twins have different irises, and each person's two irises differ from each other. The unique pattern of the human iris is fully formed by ten months of age and remains unchanged through a person's lifetime. A benefit of iris recognition is that it is not susceptible to theft, loss, or compromise, and irises are less susceptible to wear and injury than many other parts of the body. Newer iris scanners allow scanning to occur from up to ten inches away. A disadvantage of iris scanning is that some people are timid about having their eye scanned. Throughput time for this technology should also be considered. Typical throughput time is two seconds. If a number of people need to be processed through an entrance in a short period of time, this can be problematic.

3-4.9.3.7 **Retinal Scanning**. Retinal scanning is an older, comparable technology that reads the blood vessel pattern on the retina in the back of the eye, but it is not readily available in the marketplace. Whereas iris scanners can work up to ten inches from the reader, retinal scanners require individuals to look into a device that shines a harmless infrared light into the eye. Hesitance to look directly into such a reader has curtailed the acceptance of retinal scanners in most applications.

## 3-5 ACS DESIGN GUIDANCE

3-5.1 **GENERAL**. The DoD is currently migrating to the CAC. New access control system designs should be based on the CAC as the primary access control credential. Designer options for new systems are:

3-5.1.1 Current CAC technology

3-5.1.2 Future CAC technology (contactless)

3-5.1.3 Bometrics.

3-5.2 **CONSIDERATIONS**. When designing an ACS the following should be considered:

3-5.2.1 Do not design an ACS based around a single access control credential.

3-5.2.2 A coded credential alone does not offer sufficient security.

3-5.2.3 At a minimum, all card readers must be equipped with a keypad.

3-5.2.4 All card readers must be UL 294 listed and CE certified.

3-5.2.5 Contactless card readers must conform to ISO 14443 Parts 1 through 4 and NIST IR 6887, The Government Smart Card Interoperability specification (GS-IS).

3-5.2.6 For facilities requiring a higher degree of security, provide biometric capability in addition to the minimum.

Per FIPS 201, fingerprint reading is the biometric technology of choice.. Facial imaging is listed as a secondary biometric credential.

3-5.2.7 Retina scanners should not be considered as they are being phased out of the marketplace.

3-5.2.8 Outside hand-geometry readers require special exterior housings. Check with manufacturer's specifications for external applications on other biometric readers.

3-5.2.9 A common cable type for card readers is a twisted, shielded cable (typically, six conductor). One pair is used for low voltage dc power, one pair is used for data transmission, and one pair is normally used for LED or signal illumination. Verify the cable requirements with the equipment manufacturer.

3-5.2.10 Coordination with Building or Project Architect:

3-5.2.11 In general, the ESS designer must balance security requirements with life safety, fire-alarm interface, and normal operational convenience factors.

3-5.2.12 Exits and entrances should be separated.

3-5.2.13 Avoid using a life safety emergency exit as a high security entry portal.

3-5.2.14 Limit entrances into the controlled area. SCIFs are limited to one primary entrance.

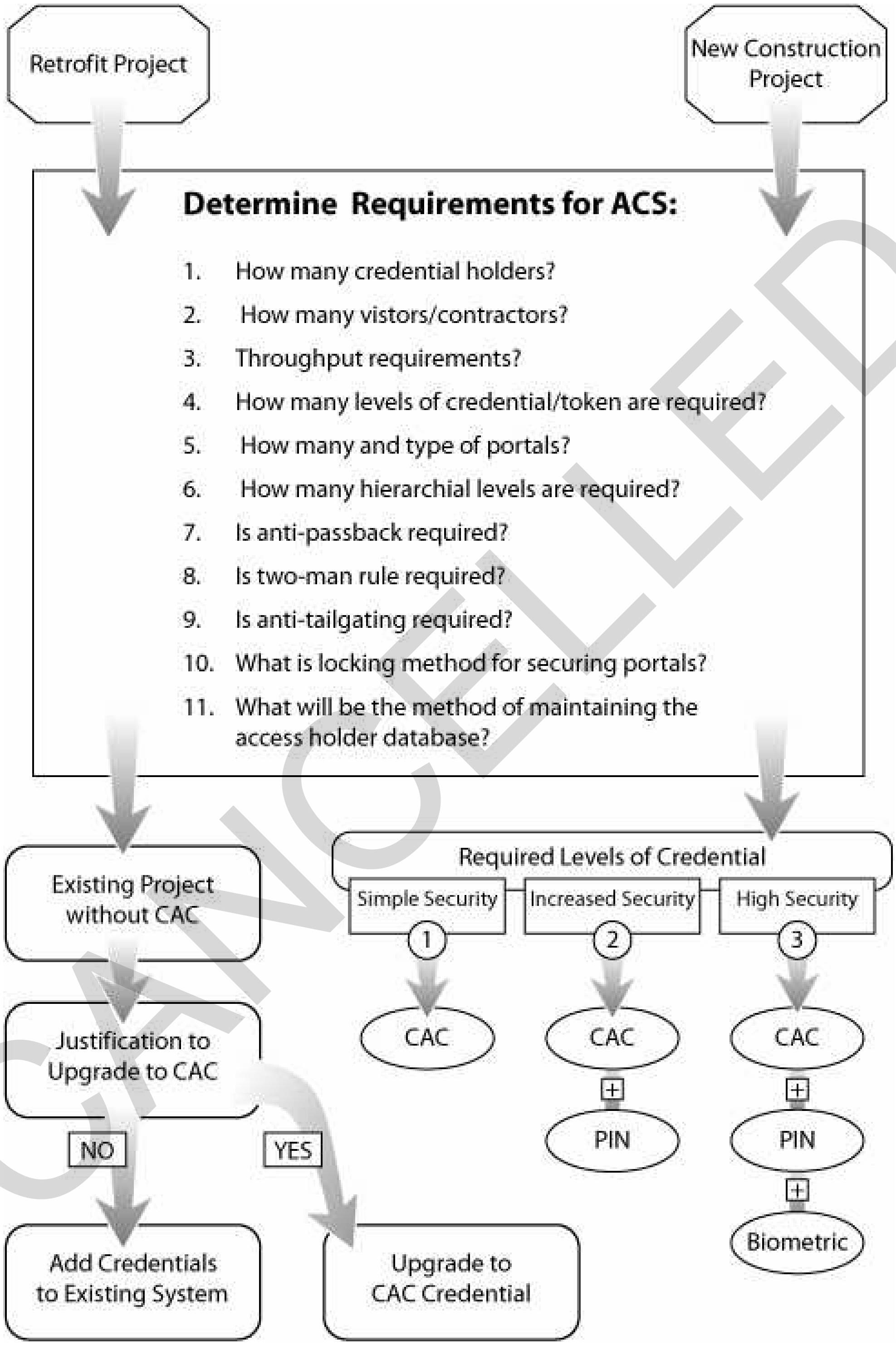
3-5.2.15 Coordinate with the Architect to ensure proper doors, door frames, and door hardware are provided. For example, when an electric strike is specified, the door and door frame should be checked or specified such that it supports the electric strike (capable of routing cables and so forth).

3-5.2.16 Consider throughput and traffic low of normal operational traffic and emergency exiting requirements. Combined credentials may result in a decrease in the false acceptance rate but will increase verification time and decrease the throughput rate.

3-5.2.17 Decide early if there are special exit technology or egress monitoring needs. Special exit technologies (request-to exit buttons or cardreaders) require life safety code consideration and additional door hardware coordination.

3-5.2.18 Additional design guidance for ACS is provided in Figure 3-8.

**Figure 3-8. ACS Design Process**


Retrofit Project
New Construction Project
Determine Requirements for ACS:
1. How many credential holders?
2. How many vistors/contractors?
3. Throughput requirements?
4. How many levels of credential/token are required?
5. How many and type of portals?
6. How many hierarchial levels are required?
7. Is anti-passback required?
8. Is two-man rule required?
9. Is anti-tailgating required?
10. What is locking method for securing portals?
11. What will be the method of maintaining the access holder database?
Existing Project without CAC
Justification to Upgrade to CAC
NO
YES
Add Credentials to Existing System
Upgrade to CAC Credential
Required Levels of Credential
Simple Security
Increased Security
High Security
1
2
3
CAC
CAC
+
PIN
CAC
+
PIN
+
Biometric

# CHAPTER 4

# CLOSED CIRCUIT TELEVISION SYSTEMS

## 4-1 OVERVIEW

4-1.1 The CCTV system is another core subsystem of an overall ESS. It is the collection of cameras, recorders, switches, keyboards, and monitors that allow viewing and recording of security events. The CCTV system is normally integrated into the overall ESS and centrally monitored at the Dispatch Center. Uses of CCTV systems for security services include several different functions as described below.

4-1.2 **Surveillance.** CCTV cameras can be used to give a viewer the capability to be made aware of or view visual events at multiple locations from a centralized remote viewing area. CCTV camera technology makes visual information available that would normally only be available through multiple (possibly roving) human resources.

4-1.3 **Assessment.** When alerted by an alarm notification, CCTV cameras allow Dispatch Center operators or other viewers to assess the situation and make a determination as to what type of response may or may not be required. An example would be an intrusion alarm at a remote facility. Visual assessment and other confirmation may indicate an unannounced maintenance crew at work. Symptoms of intrusion would lead to a response.

4-1.4 **Deterrence.** While more effective against unsophisticated burglars as opposed to trained covert insurgents, CCTV cameras may deter burglary, vandalism, or intrusion due to fear of discovery and prosecution.

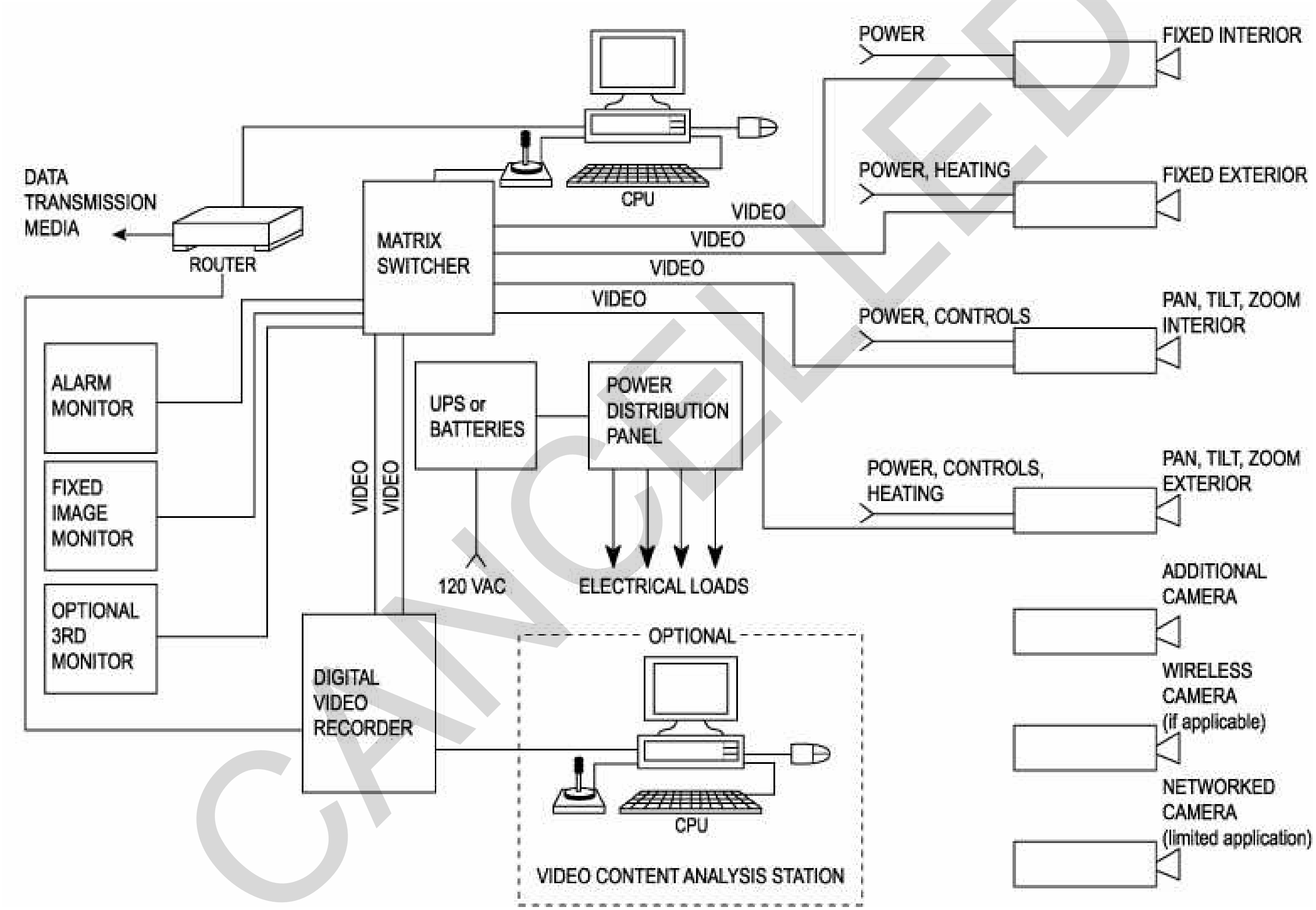
4-1.5 **Evidentiary Archives.** Retrieval of archived images may be helpful in identification or prosecution of trespassers, vandals, or other intruders.

4-1.6 **Facial Recognition.** Cameras can be used for biometric facial recognition as discussed in Chapter Three.

4-1.7 **Intrusion Detection.** CCTV cameras when employed with video content analysis or motion path analysis software and equipment are increasingly being used as a means for intrusion detection as discussed in this Chapter under *CCTV Camera Employment for Intrusion Detection.*

4-1.7.1 As shown in Figure 4-1, a CCTV system includes cameras (fixed and pan/tilt/zoom cameras for the interior and exterior of a facility, a digital video recorder, operator workstation, matrix switchers, and displays.

**Figure 4-1. Example CCTV System**



## 4-2 DIGITAL VIDEO RECORDER (DVR)

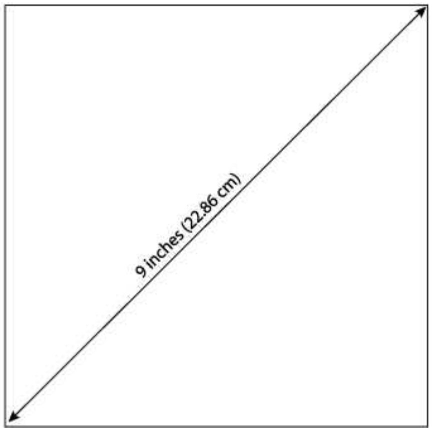
4-2.1 In current CCTV systems, the digital video recorder (DVR) has become the "heart" of the CCTV system. The DVR is used principally for the download of camera images onto a hard-drive for recording and storage of historical information. Older systems used VHS tapes, but are largely phased out. DVRs currently have memory storage capability of 80 gigabytes to 240 gigabytes with options to expand using additional hardware to increase storage. Most DVRs are provided with self-contained CD burners for archiving or removal of stored data. Most specifications call out for a CCTV system to be able to retain 30 days of camera images. The amount of storage required for 30 days is dependent on a number of factors to include: number of cameras, compression ratio, resolution, and frame rate. This subject of storage space as it relates to the above factors is developed in additional detail later in this chapter.

## 4-3 SYSTEM DISPLAYS

4-3.1 **Display Technologies.** ESS displays for CCTV images make use of three general technologies: cathode ray tube (CRT), liquid crystal display (LCD), and plasma display units. LCD and plasma display can be grouped as large format display units. A general overview on each technology follows:

4-3.2 **CRT.** CRT displays are an older technology and have been used in the security industry for a long time. A CRT works by moving an electron beam back and forth across the back of the display screen. Each time the beam makes a pass across the screen, it lights up phosphor dots on the inside of the glass tube, thereby illuminating the active portions of the screen. By drawing many such lines from the top to the bottom of the screen, it creates an entire screen full of images**.** Since individual phosphors are illuminated, the CRT technology offers a high-resolution image. There was a historic problem of a static image being "burned in" permanently on the CRT screen. Most current CRT manufacturers provide a "screen saver" image or feature to avoid this problem and extend the life of the monitor. The ESS designer should specify or verify that a screen saver feature is available for CRT displays. With a long term pedigree of security applications, security CCTV vendors offer a variety of standard CCTV monitor display sizes to include: 9, 10, 12, 14,15, 17, 19, 20, and 21 inch displays. Note that displays are described in terms of their diagonal dimension as shown in Figure 4-2. Since there has been a strong history of using CRT displays in security projects, manufacturing economies of scale have resulted in commensurate favorable COTS prices and inventory availability. While initially more cost effective as a display component, CRTs take up desk space, could require a custom built console, consume more power, and generate more heat.

**Figure 4-2. Dimensions of a "9-inch" ESS Display**



4-3.3 **Computer Monitors.** Normally supplied as CRTs, computer monitors are increasingly being used as CCTV display components. Typical sizes include 15, 17, 18, and 21 inches.

4-3.4 **LCD.** LCD displays utilize two sheets of polarizing material with a liquid crystal solution between them. The solution is liquid materials that have crystal-like properties. These materials exist as solid crystals at low temperature, but when the temperature rises they become a milky liquid and at higher temperatures, the solution becomes clear liquid. In the display assembly, an electric current passes through the crystals to align them so that light cannot pass through – thereby blocking a blacklight source. Each crystal, therefore, is like a shutter, either allowing light to pass through or blocking the light. High quality LCD displays (such as those required by ESS) use segment drivers to orient individual pixels for image generation. LCDs can be provided in either monochrome or color assembly units. LCDs commonly are provided in the 15 to 40 inch dimension range.

4-3.5 **Plasma Displays**. Plasma displays consist of two glass substrates bonded with an intermediate cell. Powering of the plasma display unit results in a high-quality image on the display side of a color filter unit. The displays are programmable and can display multiple images in a matrix format. Common plasma display sizes range from 42 to 84 inches.

4-3.6 **Summary**. Due to a past history of being the workhorse for security display needs, CRTs are readily available through security vendors as a standard product offering competitive prices, available inventories, and standardized dedicated conductor connections. As another variant of CRT screens, for small quantities of cameras, use of PC monitors are being used. With PC based video presentation, it is not important to constrain the matrix to a square. The display can be dynamically sized based on events. New developments in large format displays offer advantages of consuming less space, consuming less power, and offering greater flexibility in display format. In addition to requiring less power and space, large format displays offer the advantage of little to no glare off the display screen. Currently, large format displays are usually made and offered by flat panel suppliers and need to integrated into a CCTV display system.

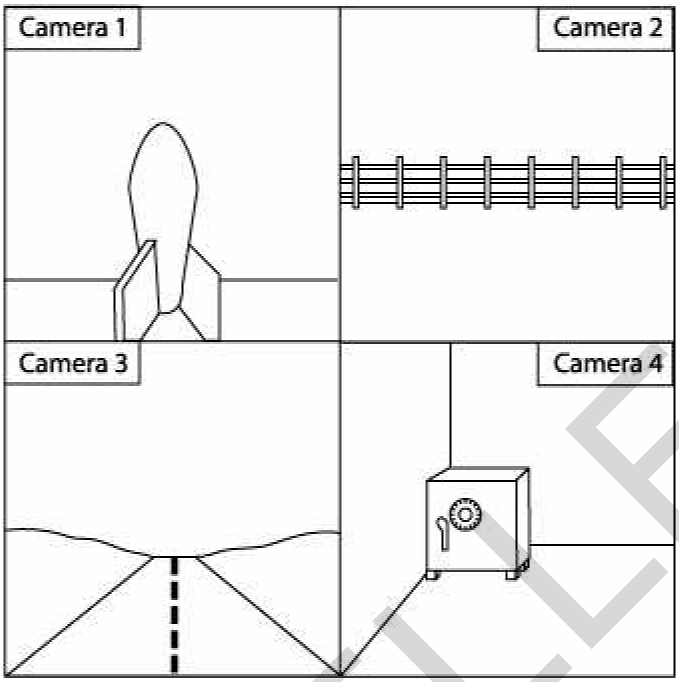
4-3.7 **Display Setups.** There are a variety of methods to display images as described below:

4-3.8 **Single Image Display**. A single CCTV camera image is displayed. This is best used for a single dedicated camera that is critical for monitoring. Nine inches (9 inches: 22.86 cm) is the smallest screen recommended for displaying a single camera image.

4-3.9 **Split-Screen.** “Split-screen” is most commonly used to describe displaying multiple CCTV camera images on a single display. The display screen is typically split into a square pattern. Fifteen inches (15 inches: 38.1 cm) is the smallest sized recommended for split screen viewing for up to a maximum of four cameras. More than four camera images on a 15-inch display become too small to see. Figure 4-3 shows four camera images on a single 15-inch display.

4-3.10 **Matrix Displaying for Large Format Displays**. LCD and flat-screen plasma displays lend themselves to programming to show several camera images. The configuration is best done in a square matrix (for example 9 images in a 3 by 3 matrix or 25 images in a 5 by 5 matrix). A square matrix avoids distorting or stretching the camera image in one direction or the other as would occur in a 5 by 7 matrix configuration.

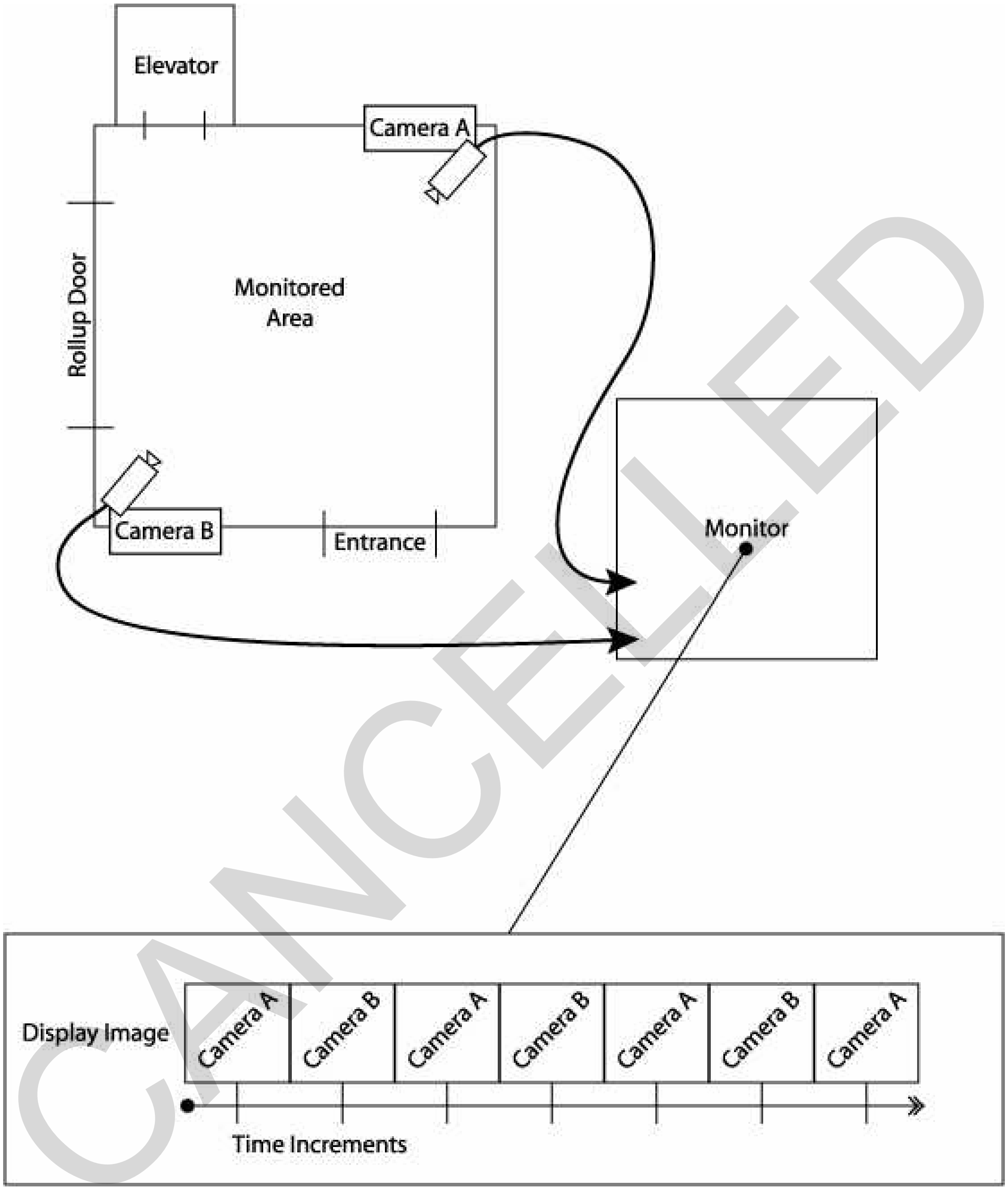
**Figure 4-3. Example of a "Quad-Screen" Display**



4-3.11 Switching Display uses time programming to show different camera images on the same display. An example of "switching" would be a single CRT display to display alternating images from two different cameras. An application would be using a single monitor to display alternating images of two cameras at five seconds duration each. The sequence would be to display the Camera A for five seconds, followed by a display of the Camera B image for five seconds, followed by Camera A for five second, and so on as shown in Figure 4-4.

4-3.12 Table 4-1 provides CCTV-display component application guidance.

**Figure 4-4. “Switching” Two Camera Images on a Single Display**



4-3.12.1 Figure 4-4 is a rudimentary example of a switching display. The diagram is taken from an actual project, where coverage of possible camera “dead zones” from a single camera was needed. The solution was to add a second camera. More complex display systems use a display switcher to monitor and scan multiple cameras. The “switcher” determines the duration that the monitor views a specific camera.

**Table 4-1. CCTV-Display Component Application Guidance**

| Use This Equipment | For This Reason |
|---|---|
| Black and white (monochrome) display | When color information is not required.<br>Some Video Content Analysis systems only work with black and white cameras. |
| Color displays | When color information such as clothing or vehicle color specifics are needed. |
| CRT displays | When the space configuration lends itself to addition of console mounted-type displays. |
| LCD Displays | Lower power consumption<br>Less space required<br>Higher resolution. |
| Large-format display, 23 inches to 80 inches or larger | • When overall dispatch center (console and desk) space is limited.  (Assumes wall-mounted or suspended displays.)<br>• When having  little glare from the display is a significant concern.<br>• When power consumption is a significant consideration.<br>• When a large number of displays (more than nine in matrix fashion) are required.<br>• When flexibility of programming images is required. |

4-3.13 Banks of CCTV monitors increase cost. Designs should consider having one monitor for “alarm call-up” and additional monitors for a fixed view or switching images. The tenant command or ESS Project Manager should be wary of the vendor advocating a monitor for every camera. Individual project display configurations will vary based on the nature of the project specifics such as number of critical assets, criticality of the asset, number of CCTV cameras, and space allocation. Figures 4-5 through 4-7 illustrate three different possible configurations. Figure 4-5 is a basic simple project configuration. Figure 4-6 displays static images for a twenty-five camera project. Figure 4-7 illustrates a robust display configuration that allows viewing of pre-alarm, current situation, and post-alarm images for a single event. In Figure 4-7, pre-alarm shows the events shortly before the ESS alarm. Conversely, the post-alarm displays the events shortly after the ESS alarm.

**Figure 4-5. Simple Two Display Monitor Configuration**

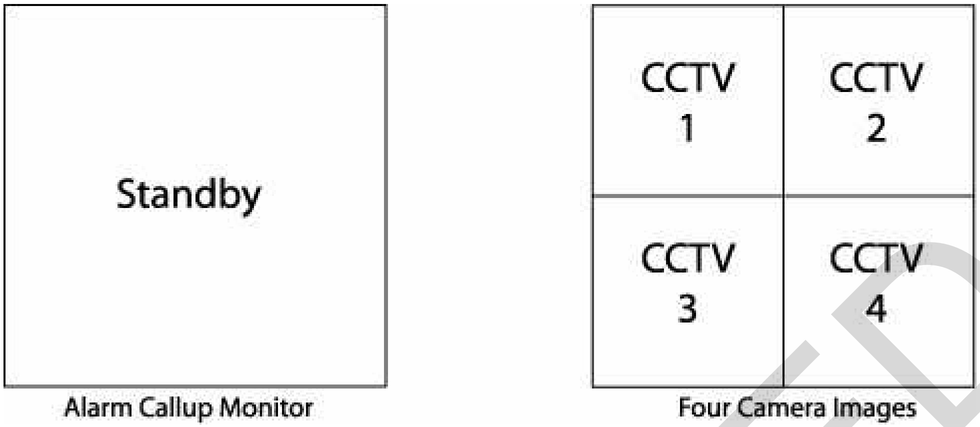


**Figure 4-6. Multiple Images on A Single Display**

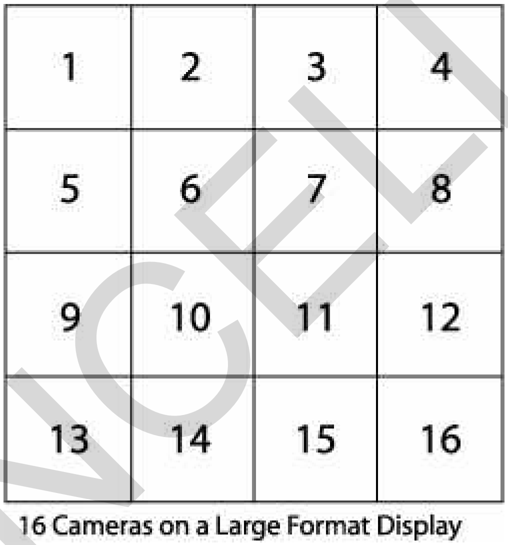
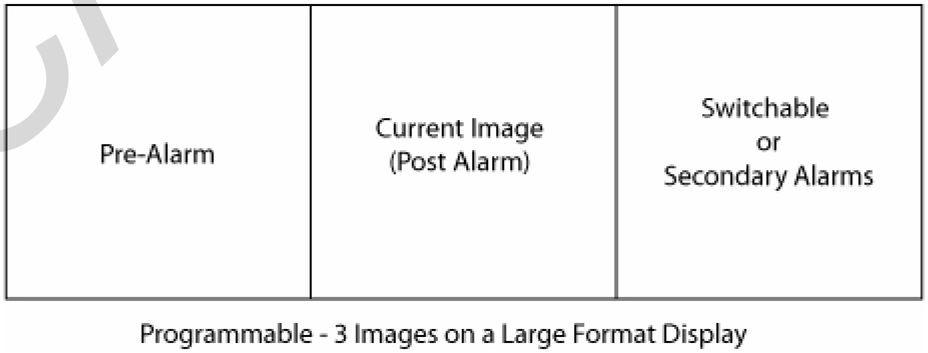


**Figure 4-7. Pre-alarm, Current, and Post-Alarm Image Comparison**



## 4-4 VIDEO MATRIX SWITCHERS

4-4.1 Video matrix switchers are components that provide switching capability between cameras and viewing monitor displays. They typically offer functionality that allows programmable settings such as loss of video alarms, camera naming, guard-tour camera sequences, and salvo switching, which activates several cameras simultaneously to pre-set views. Video matrix switchers can simultaneously switch pan/tilt/zoom (PTZ) control signals with the video, so that control follows the active camera.

## 4-5 KEYBOARDS

4-5.1 Keyboards allow an operator to control pan/tilt/zoom cameras. They are also used to identify which camera to call up and display on the screen. Some CCTV system keyboards come with “track balls” or joy sticks that facilitate camera control.

## 4-6 CAMERAS

4-6.1 **Color versus Black and White**. Color cameras offer more information such as color of a vehicle or subject’s clothing. Some ultra-low light color cameras are able to automatically sense the ambient light conditions and switch from color to black and white in low light conditions. Cameras must have auto-white balance to adjust for the changing color temperature of daylight and artificial lighting needed for night-time viewing. Black and white cameras are more sensitive under low-light or darkness conditions and are best used when IR illuminators are required**.** These cameras are further described in the *Viewing in Low-Light Conditions* Section of this chapter.

4-6.1.1 Color cameras require a higher illumination level than black and white cameras to be effective. Typically, a high-quality color camera will work well down to 1.5 footcandle (fc) illumination, whereas a standard black and white camera might only require 0.5 fc. These lighting level requirements vary with the camera model and manufacturer, so be sure to specify the necessary illumination level that is required for camera observation, and coordinate carefully with the lighting levels for the particular area to be viewed.

4-6.2 **Indoor Cameras**. Indoor camera installations reduce the complexity of the system, but care must be taken to correctly specify the lens, field-of-view and camera hardware. Indoor cameras need:

4-6.2.1 Sturdy, secure mounting.

4-6.2.2 Auto-iris for lighting control.

4-6.2.3 Auto-white balance to ensure proper color correction to accommodate changes in color temperature of lighting if it is dimmed or lighting is changed due to a light outage.

4-6.2.4 To be mounted in a position to prevent glare to the lens from overhead lighting.

4-6.2.5 Manual adjustment that the operator at the monitor station can use to accommodate backlighting situations caused in situations such as when a camera faces a door to the outside with too much light coming to the camera lens, causing a backlight situation.

4-6.3 **Outdoor Cameras**. Outdoor camera installations cost more than indoor cameras due to the need to environmentally house, heat, and ventilate the outside camera. When mounting a camera outdoors, the lighting requirement changes depending on the time of day and the weather. Because of this, consider the following for outdoor cameras:

4-6.3.1 Shrubs, trees, and other vegetation in a camera's line of sight may cause obstructed views. Designers need to be aware of this when determining where to place cameras. Also, motion detector systems can register a false positive when plants in the field-of-view move in windy conditions.

4-6.3.2 Provide heaters in cold weather applications.

4-6.3.3 Always use auto-iris lenses with outdoor cameras. The iris automatically adjusts the amount of light reaching the camera and thereby optimizes its performance. The iris also protects the image sensor from getting damaged by strong sunlight. Always set the focus in low light with an auto-iris lens. If the adjustment is made in sunlight, it is very easy to focus, but at night the iris diameter increases and the image is not in focus anymore. Special dark focus filters called "neutral density" filters or ND filters help reduce lighting by one or more stops of exposure. These filters do not affect the color of the image.

4-6.3.4 Use caution when mounting a camera behind glass. If you mount a camera behind glass, such as in a housing, make sure that the lens is close to the glass. If the lens is too far away from the glass, reflections from the camera and the background will appear in the image.

4-6.3.5 Always try to avoid direct sunlight in an image. Direct sunlight blinds the camera and may permanently bleach the small color filters on the sensor chip, causing stripes in the image. If possible, position the camera so that it is looking in the same direction as the sun.

4-6.3.6 When using a camera outdoors, avoid viewing too much sky. Due to the large contrast, the camera will adjust to achieve a good light level for the sky, and the landscape and objects that must be assessed might appear too dark. One way to avoid these problems is to mount the camera high above ground. Use a pole if needed. Given mounting choices, mount cameras facing away from rising or setting sun, realizing that this varies by season.

4-6.3.7 Always use sturdy mounting equipment to avoid vibrations caused by strong wind. This is especially important with a long focal length lens. These lenses amplify even the smallest movement of the mount. Building mounts are generally more stable than pole mounts. When in extremely windy conditions for a critical camera, consider using a gyro-stabilized mount lens to avoid vibration caused by wind. The gyro-stabilized lens has a cost premium and is not appropriate for general applications.

4-6.4 **Fixed Position Cameras**. Fixed position cameras are mounted in a fixed position and cannot rotate or pan. A good application for fixed cameras is *detection* surveillance, because video motion detection can be more readily applied to the static field-of-view. The installation and cost of fixed cameras is lower because there is no associated motor/control wiring. Fixed cameras are good for review of pre-alarm conditions because there is a static view of the alarm area. Pre-alarm allows the review of video information for the time period (typically ten to fifteen seconds) immediately before the alarm occurred. Due to the static view, fixed cameras are not as well suited for tracking a dynamic event.

4-6.5 **Pan/Tilt/Zoom (PTZ) Cameras**. PTZ camera mounts allow the camera to rotate, pan, tilt, and zoom. Because of the drive motor, housing, and wiring for controls, PTZ cameras are typically three to four times more expensive than fixed cameras. However, the operator gets a much better view of the overall area than with a fixed camera. PTZ cameras are often used for assessment surveillance applications to view and assess alarm conditions. PTZ cameras are not well-suited for pre-alarm assessment because they may not be focused on the alarm area at all times. When designing CCTV surveillance, consideration needs to be given to lost coverage within the camera sweep field-of-view when the camera zooms to a fixed location. Refer to Figure 4-8.

4-6.5.1 There are three modes in which PTZ cameras can be employed:

4-6.5.1.1 Default at home and zoom to alarm.

4-6.5.1.2 Continually sweep

4-6.5.1.3 Manual control

Figure 4-8. PTZ Sweep Range

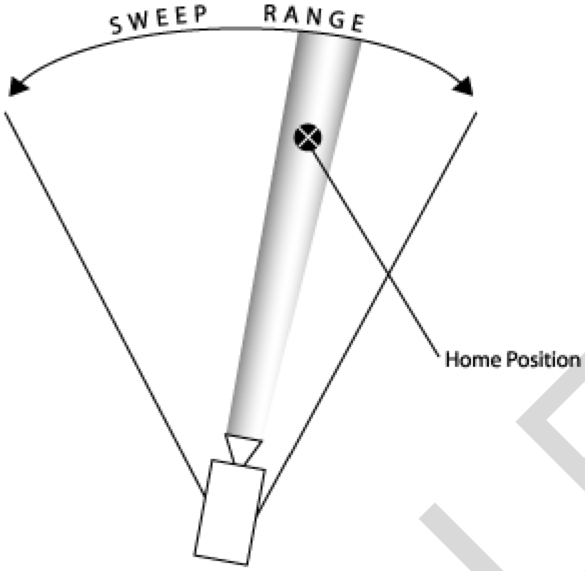


Table 4-2. Fixed versus PTZ Cameras

| | Applications | Cost | Pre-alarm Review | Video Motion Detection | Intruder Tracking Capability |
|---|---|---|---|---|---|
| **Fixed** | Fixed assets such as doors, entry gates, and loading docks | Lower | Recommended | Recommended | None |
| **PTZ** | Open areas, fencelines | Three times more expensive than a fixed camera | Poor application | Poor application | Good |

4-6.6 **Dome Cameras**. Dome cameras are actually a cheaper version of the PTZ camera when the total cost is considered (installation, parts, and maintenance). Dome cameras are mounted in a hardened plastic lower-dome, which is commonly smoked-colored to conceal the camera. The use of smoke-colored domes provides covert lens positioning, while the use of clear domes provides for better low-light performance. Dome cameras are a good design solution for applications where the camera needs to be protected from the environment (such as dust) or it is desired to conceal the axis and field-of-view for a scanning camera. A common application of dome cameras is in office buildings with suspended ceilings. The dome camera is more aesthetic and less “harsh” looking than a camera unit. Improvements in product design have reduced the packing to integral units that now fit in the space of a quarter ceiling tile. PTZ features within dome cameras move substantially quicker than conventional cameras with a separate PTZ drive unit on them.

4-6.7 **Cost Considerations**. The obvious primary cost considerations are the number of cameras, mounting devices, and the associated wiring. Adding more cameras will increase the personnel burden required for monitoring those cameras. This can be alleviated by the proper design of a monitoring system. If cameras are not monitored, their data should be recorded and stored for use as after-the-fact evidence. As discussed in the *System Displays* Section, larger plasma panels or flat screen displays can be configured to show only cameras that display alarm conditions.

4-6.7.1 **Effect on maintenance costs.** In general, more cameras and more monitoring systems are going to result in higher maintenance costs.

4-6.7.2 **Order of magnitude cost estimates.** While there will be variations with actual installed constructed cost across the United States based on labor type (union or nonunion) and labor supply, the following general rules of thumb can be used for conceptual cost estimating:

4-6.7.3 Interior fixed camera: $2,100

4-6.7.4 Interior speed dome camera: $3,800

4-6.7.5 Exterior fixed camera with heating equipment: $5,600

4-6.7.6 Exterior, pan-tilt-zoom camera: $7,600

## 4-7 INTERNET PROTOCOL (IP) ADDRESSABLE CAMERAS

4-7.1 An IP camera captures a video image digitally. The video encoder protocols have not been standardized within the security industry and therefore these cameras require up-front care in specifying the correct protocol and viewing software.

4-7.2 **Typical System Configuration**. The IP camera resides on a local area network (LAN). Video data is transmitted via the LAN to a video server that routes the video to end-users and possible mass storage devices (storage server).

4-7.3 **Pros and Cons**. IP cameras are the least secure CCTV system, but may have application where remote viewing over a network is desired, or where a high-bandwidth network may exist. For example, with a typical matrix switcher configuration, in order to view camera images at a site distant from the actual matrix switcher location, new cabling must be run between the matrix switcher and the remote site. With an IP camera system, a network connection between the sites is all that is required to view any camera image on the system. One drawback to IP cameras is that they cost more than a standard analog (non-IP) camera. Due to the security concerns with the internet, IP cameras will generally not be used on DoD projects. The possible exception would be CCTV surveillance of low priority assets at remote locations.

## 4-8 RECORDING

4-8.1 Recording of CCTV images is almost always done for retrieval of surveillance information**.** Consideration must be given to the location and capacity of the recorders**.** The bandwidth requirements for streaming video can be high (i.e. 3.07 Mbps for one camera in alarm.) To reduce recurring cost of transmitting high bandwidth demands, it is a good design practice to install recording equipment locally and transmit lower quality images back to the Dispatch Center. For example, it is less costly to download camera images at 15 frames per second (fps) at the local site and transmit a 2 fps image back to the Dispatch Center. While the 2 fps image will be choppier, it can give sufficient information to view what is going on at a remote site (i.e. there is an intruder). If evidentiary information (i.e. identity of the intruder) is required that information can be retrieved from the local site. Alternatively, more time can be used to download a higher quality image if so needed.

4-8.2 **Storage Requirements**. This example demonstrates how to calculate storage requirements. Assuming a typical camera image of 25 kbytes, the required memory storage capability for 30 days of images at 6 frames per second is 389 Gb. That storage requirement is calculated in Figure 4-9.

**Figure 4-9. Calculation for Storage of Frame Size of 25 kbytes**

Capacity = (Frame file size in bytes) x (frames per second) x (duration in seconds)

Capacity = 25 kbytes x (6 frames per second) x (3600 sec/hr) = 540 Mb x (24 hr/day) x 30 days = 389 Gb

Thus, one camera transmitting camera images of 25 kbytes in size will require 389 Gb for 30 days of storage.

4-8.2.1 Quickly, it can be seen the memory requirements for a complex camera system can be extensive**.** The ESS designer needs to specify sufficient recording media/methods to archive the project's camera images using a methodology similar to the one displayed in Figure 4-9.

4-8.3 **Principle Technologies**. There are four principal technologies for recording CCTV video information: old-fashioned VHS, contemporary digital video recorders (DVRs), network video storage, and data servers.

4-8.3.1 **VHS Recording** is an older technology. Banks of VHS recorders were designed to download CCTV camera images. Tapes were frequently swapped out and storage space had to be planned for record retention. Since VHS technology has been made obsolete by current technology (i.e. DVRs), VHS units are not recommended for new security projects.

4-8.3.2 **Digital Video Recorders**. Digital video recording provides a great improvement in camera image storage. Benefits include eliminating consumable media (tapes), reducing physical storage space, ease of search-and-playback functions, and the capability to add watermarks for documenting evidentiary recordings.

4-8.3.3 **Network Video Storage**. An emerging trend in modern CCTV systems is the capability to use network storage for video images. This enables the use of standard hard disk arrays, such as a redundant array of independent disks (more commonly known as a RAID array), a system of using multiple hard drives for sharing or replicating data among the drives. The benefit of RAID over using drives singularly is increased data integrity, fault-tolerance, and/or performance**.** RAID arrays offer the use of any standard storage hardware instead of using a proprietary digital video recorder unit(s).

4-8.3.4 **Data Servers**. With the development of telecommunications equipment and an oversupply of associated data centers, new companies are seeking novel market opportunities for data storage. The trend in the industry is that a few specialized data storage companies, that have the unique telecommunications engineering experience and capital to build data centers or “server farms,” are offering out-sourced data storage services in the Terabit or Petabit range. While not totally mature, it can be expected that secure methods of CCTV images will be the way of the future for CCTV security systems.

## 4-9 ILLUMINATION

4-9.1 A significant part of visibility is lighting. Lighting should enable parking lot personnel and employees to note individuals at night at a distance of 75 feet or more and to identify a human face at about 33 feet. These are distances that will allow them, if necessary, to avoid the individuals or take defensive action while still at a safe distance. Security lighting increases the effectiveness of guard forces and closed circuit television by increasing the visual range of the guards or CCTV during periods of darkness. It also provides increased illumination of an area where natural light does not reach or is insufficient. Lighting also has value as a deterrent to individuals looking for an opportunity to commit crime. Normally, security lighting requires less intensity than lighting in working areas. An exception is at normal doorways.

4-9.1.1 Refer to UFC 3-530-01, Interior, Exterior Lighting and Controls for general lighting guidelines. Refer to MIL-HDBK-1013/1A Design Guidelines for Physical Security of Facilities for security lighting requirements.

4-9.2 **Interior Lighting.** Interior lighting for CCTV presents special issues that need to be considered by the designer. For example, after-hours lighting may be significantly lower than normal operation lighting. Two solutions help minimize this impact.

4-9.2.1 The first technique is the use of cameras with automatic backlight compensation. Backlight compensation is a camera feature that enables the camera to automatically adjust picture brightness depending on lighting conditions, which compensates for bright backgrounds so foreground objects are not silhouetted. Frequently, CCTV cameras near windows are affected by backlighting, causing shadows and silhouettes, so the use of appropriate cameras with backlight compensation is effective.

4-9.2.2 The second technique is the use of cameras with automatic gain control, a feature that amplifies existing video to help camera create an enhanced video signal at low light levels.

4-9.2.3 Both of these techniques enable cameras to function more effectively in interior low-light conditions, and are also useful for outdoor cameras as well. In some cases, the integration of CCTV cameras with night-lights and intrusion sensors can be very effective. The sequence of events might be as follows: an intruder activates an interior presence sensor, which in turn activates instant-on lighting or a night-light, and the CCTV camera is triggered and video images are recorded.

4-9.3 **Light-to-Dark Ratio.** One design parameter of CCTV systems is specification of a proper light-to-dark ratio in the space viewed. "Light-to-dark" ratio refers to the light intensity (as measured in foot-candles or LUX) of the lightest (most reflective surface) to the darkest (least reflective surface). A proper light-to-dark ratio for good CCTV picture clarity is 4:1. The maximum ratio is 8:1. When the ratio is too high, the shadows appear black and the viewer can not distinguish any shapes in the shadows. While not always achievable, the designer should strive for a light-to-dark ratio of 4:1, as shown in Table 4-3. For guidance on light sources and lighting levels, refer to UFC 3-530-01.

**Table 4-3. Light-to-Dark Ratios**

| Light-to-Dark Ratio | Quality of Image |
|---|---|
| 4:1 | Great |
| 6:1 | Good |
| 8:1 | Marginally acceptable |

4-9.3.1 The CCTV system designer can influence the light-to-dark ratio by coordinating with the project's lighting engineer, landscape engineer and interior designer. Actions the designer can take to achieve a proper light-to-dark ratio include:

4-9.3.1.1 Positioning of lighting.

4-9.3.1.2 Positioning of cameras.

4-9.3.2 When cameras and lights are mounted in close proximity, take care that the light does not interfere with the field-of-view of the camera, such that glare or backlighting issues do not occur.

4-9.3.3 Adjusting the field-of-view.

4-9.3.4 Selecting building surface interiors to minimize contrasts

4-9.3.5 Engagement of lighting engineers for new construction projects allows modeling of light-to-dark ratios for different material selection; such as concrete versus drywall. For retrofit projects, the same modeling approach can be applied, but requires changing existing surfaces or modifying lighting sources and locations.

## 4-10 VIEWING IN LOW-LIGHT CONDITIONS

4-10.1 In addition to increasing the illumination level of the surrounding area, several technology solutions are available to permit viewing under low-light conditions. These include black/white switching cameras, infrared illuminators, or thermal imagers. These technologies are often used where visible light either brings undesired attention to a critical facility, or surrounding property owners object to visible light adequate for good visual camera operation.

4-10.2 **Black/White Switching**. Some cameras will automatically switch from color during daytime to black/white at night, which permits viewing under low light conditions. This can be an effective solution in situations where the existing illumination levels are too low during night conditions to permit color camera use, but color camera use is desired during daytime conditions. Numerous CCTV camera manufacturers offer auto-switching black/white cameras.

4-10.3 **Infrared Illuminators**. The human eye cannot see infrared light. Most monochrome CCTV (black/white) cameras, however, can. Thus, invisible infrared light can be used to illuminate a scene, which allows night surveillance without the need for additional artificial lighting. Infrared also provides many other benefits above conventional lighting, including:

4-10.3.1 IR beam-shapes can be designed to optimize CCTV camera performance

4-10.3.2 Extended bulb-life

4-10.3.3 Covert surveillance, no visible lighting to alert or annoy neighbors

4-10.3.4 Lower running costs (but higher installation costs)

4-10.3.5 Ranges at which illuminators are effective vary with manufacturer and model. Typical values are 10 meters to 85 meters.

4-10.3.5.1 It is important to design illumination specifically for the CCTV camera being used. For example, infrared illuminators require black/white cameras and do not work on color cameras. The range that the camera will see in the dark depends on sensitivity and spectral response of the camera and lens combination. Color cameras will not accurately reproduce color images when used under infrared illumination. Many black and white cameras use infrared filters to intentionally filter out non-visible light. Therefore, black and white cameras which are designed to be used in conjunction with infrared lighting should be specified such that there is not infrared filter. Dual mode cameras that can switch from color to monochrome operation in low light conditions should also have any infrared filter removed for the reason cited above.

4-10.3.6 A number of illuminator manufacturers each produce a variety of beam patterns. For example 10° and 30° spot (precise) illuminators and 60° flood illuminators.

4-10.4 **Thermal Imagers**. Thermal imagers use a special technology that senses heat signatures rather than visual information. These cameras operate under complete darkness. Thermal imagers are best used in long-range detection and surveillance applications. Thermal imagers detect and display images based on infrared light emitted from objects rather than visible light reflected off objects. The most common technology is Forward Looking Infrared (FLIR). Thermal cameras work on a temperature differential between the object and the background. In desert environments, the background is white and people are black. In cooler environments, the background is black and people are shown as white images. A key advantage of long-range thermal imagers is that they are less susceptible to environmental influences from rain and fog. The disadvantage of thermal-imagers is the high cost. Typically thermal imagers are classified as medium or long wavelength as illustrated in Table 4-4.

**Table 4-4. Characteristics of Thermal Imagers**

| **Classification** | **Wavelength** | **Cooling** | **Cost** | **Recommended Service Period** |
|---|---|---|---|---|
| **Medium** | 3- 5 micron meters | Cryogenically cooled. | $100K | 7500 hours |
| **Long** | 7-14 micron meters | Uncooled | $70K | 30,000 hours |

## 4-11 POWER

4-11.1 Options for CCTV power include 12 Vdc, 24 Vdc, 24 VAC, and 120 VAC. As with any power system, it is important to understand voltage drop limitations, current draw issues, grounding, and battery or uninterruptable power supply (UPS) backup. Exterior camera are typically powered by 120 VAC because additional power is needed for heating and controls (pan, tilt, zoom). 12 Vdc and 24 Vdc cameras are easier to provide backup power with through batteries. Power systems are further described in Chapter 9, “General Requirements and Cross-Discipline Coordination.”

## 4-12 CAMERA FIELDS-OF-VIEW

4-12.1 An important consideration when designing a camera system is determining the field-of-view for each camera. The camera field-of-view affects the lens, zoom level, and number of cameras needed.

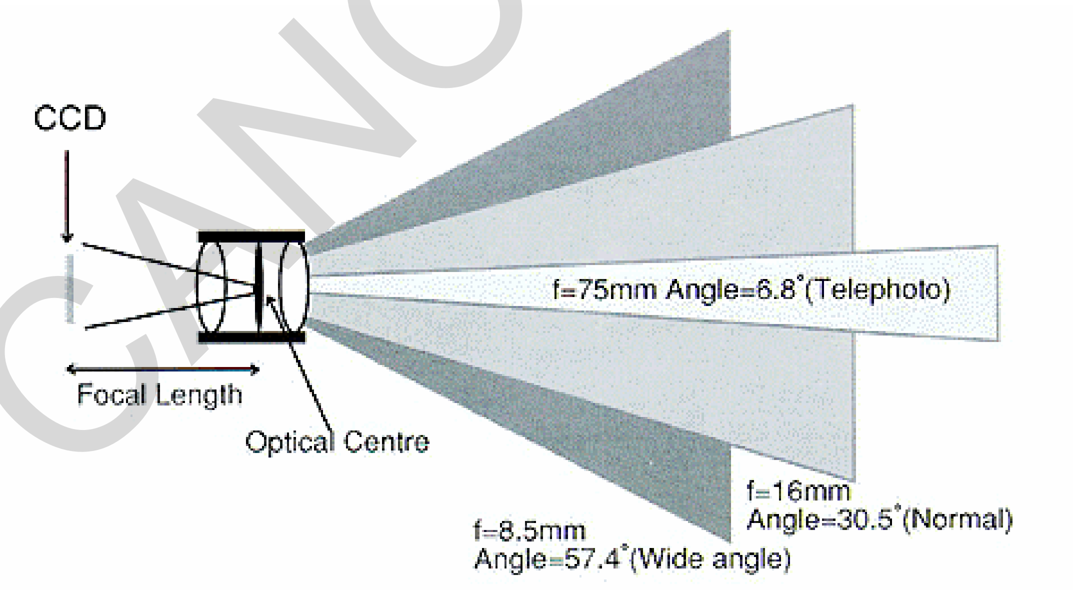
4-12.2 For cameras used to *detect* an intruder (with the capability to determine the presence of an intruder but not necessarily classify the intruder as a human, animal or object), the area of interest should occupy a minimum of 10 percent of the field-of-view, with a maximum field-of-view of 300 feet in length or less.

4-12.3 For cameras used for *classification* of an intruder (the capability to classify an intruder as human), the area of interest should occupy a minimum of 15 to 20 percent of the field-of-view, with a maximum field-of-view of 200 feet in length or less. The lens selection and alignment should be established so that the field-of-view should be no more than 150 feet wide at the far end of the alarm sector to allow at least 4.5 pixels to cover a 1-foot square target. That minimum resolution is needed to classify the intrusion source as being a person versus an animal or debris. This likely requires that the camera be mounted outside the zone being assessed.

4-12.4 For cameras used for *identification* of an intruder (the capability to determine the identity of a human intruder), the area of interest should occupy a minimum of 25 percent of the field-of-view, with a maximum field-of-view of 75 feet in length or less.

4-12.5 Figure 4-10 compares the field-of-view of a telephoto lens with that of a normal human eye and a wide-angle lens. For short focal lengths, a wide angle lens is appropriate. It will, however, provide lower magnification. For long focal lengths, a telephoto lens is appropriate. It will, however, provide a narrow field-of-view. Note that a normal human eye sees at a 30.5° angle. In Figure 4-11, “CCD” refers to “charge-coupled device,” which is the main microelectronic chip that makes up the camera unit. The charge-coupled device (CCD) is a sensor that collects light and turns it into an electronic signal. Typical CCD sizes include 1/3-inch and ½-inch devices. The larger the device, the more the area the sensor occupies and (typically) the greater the image resolution.

**Figure 4-10. Relative Magnification of an Object**



4-12.6 Figure 4-11 shows the relationship between field-of-view and the focal length of a lens. Select an appropriate focal length and use this formula to calculate image field-of-view:

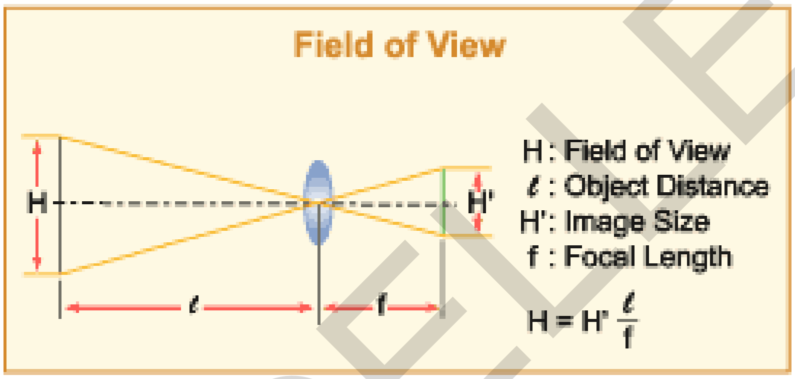
4-12.6.1 Select the focal length (f).

4-12.6.2 Estimate the image size desired (H’).

4-12.6.3 Estimate the maximum object distance (l).

4-12.6.4 Calculate the field-of-view (H): H= H’x(l/f).

**Figure 4-11. Field-of-view and Focal Length**



4-12.7 For example, a 2 meter high person would generate a 0.32 millimeter image size when 100 meters away from a camera with a 16 milimeter focal length.

2 meter person (H) = H’ image size x 100 meters (l)/16 milimeters (f).

H’ = 2 meter person x 16 milimeters/100 meters.

H’= 0.32 milimeter image/person on the camera.

The image size in the monitor depends on the display size.

## 4-13 RESOLUTION

4-13.1 Resolution refers to the “graininess” of an image**.** A sharp picture has more pixels of information and is viewed as a “sharp” picture**.** Less pixels (digital cameras) or TV lines (analog cameras) will result in a “grainier” image**.** 640 pixels by 480 pixels is an industry standard resolution for digital cameras**.** 320 by 240 will generate a satisfactory image that can help with transmission costs because it is a quarter of the data associated with a 640 by 480 image. The system designer is recommended to use 640 by 480 as a standard CCTV resolution design criterion for digital cameras**.** As a minimum, use 320 by 240 if there are bandwidth issues. For analog cameras, use 480 TV lines (high) to 330 TV lines (low).

## 4-14 FRAMES PER SECOND (FPS)

4-14.1 CCTV cameras transmit video in image frames. The measure of the “smoothness” of the playback of the video is quantified in frames per second (fps). Television video is displayed at 30 fps. For most security applications, 30 fps is higher than needed for evidentiary and investigative purposes. Additionally, CCTV cameras have the option to transmit video at two image rates: alarm condition and non-alarm condition. Making use of a lower non-alarm fps can reduce project cost by allowing a lower bandwidth transmission and storage requirement (recording) of the CCTV system.

4-14.2 Non-alarm frame speeds can fall in the 1 fps to 5 fps range (3 fps average).

4-14.3 Alarm condition frame speeds can fall in the 10 fps to 20 fps (15 fps average).

## 4-15 BANDWIDTH

4-15.1 In general, the bandwidth required increases with the frame rate used. Use this formula to calculate bandwidth:

Bandwidth = (pixels horizontal by vertical) * (frame rate in images/sec)

4-15.2 Sample calculations for a camera in nonalarm mode at 2 fps (Figure 4-12) and in alarm mode at 10 fps (Figure 4-13) are provided to demonstrate the impact on CCTV communication bandwidth requirements. The following assumptions apply for the calculations:

4-15.2.1 Assumption #1: Resolution is 640 pixels by 480 pixels

4-15.2.2 Assumption #2: Compression ratio is 20:1

**Figure 4-12. Calculation For a Camera in Nonalarm Mode at 2 FPS**

- At 2 bytes/pixel = 614,400 bytes, or 614.4 kb, per image.
- Compression: 614.4kb per second (kpbs/20) = 30.7 kbps per image frame.
- Camera rate is 2 frames/sec = 2 x 30.7 kbps = 61.4 kbps.
- Convert bytes to bits (8bits/bytes + 2 control bits = 10 bits/byte)
- Bandwidth = 61.4 kbps = 0.61 megabytes per second (Mbps).

Thus one camera in normal (nonalarm) monitoring transmits video at a bandwidth of **0.61 Mbps.**

**Figure 4-13. Calculation For a Camera in Alarm Mode at 10 fps**

- At 2 bytes/pixel = 614,400 bytes, or 614.4 kb, per image.
- Compression:  614.4kb per second (kpbs/20) = 30.7 kbps per image frame.
- Camera rate is 10 frames/sec = 10 x 30.7 kbps = 307 kbps.
- Convert bytes to bits (8bits/bytes + 2 control bits = 10 bits/byte)
- Bandwidth = 307 kbps = 3.07 megabytes per second (Mbps).

Thus one camera in alarm monitoring transmits video at a bandwidth of **3.07 Mbps.**

4-15.3 **Compression.** Digital images and digital video can be compressed in order to save space on hard drives and make transmission faster. Typically, the compression ratio is between 10 and 100. Different encoding/decoding (codec) schemes are used such as:

4-15.3.1 M-JPEG (Joint Photographic Experts Group, Motion Picture) is a compression technique for color images and photographs that balances compression against loss of detail in the image. The greater the compression, the more information is lost. MJPEG can be provided in any resolution size.

4-15.3.2 MPEG-1 (Motion Picture Experts Group) is the first MPEG format for compressed video, optimized for CD-ROM. MPEG was designed for transmission rates of approximately 1.5 Mbps. MPEG-1 encoding can introduce blockiness, color bleed, and shimmering effects on video and lack of detail on audio. Typical MPEG-1 resolution sizes are 352 x 240 pixels and 320 x 240 pixels.

4-15.3.3 MPEG2 is a variant of MPEG1 that is optimized for broadcast quality video and high-definition TV. Typical MPEG-2 resolution sizes are 720 x 240 pixels and 640 x 480 pixels.

4-15.3.4 MPEG4 is based on MPEG-1 and MPEG-2. MPEG-4 files are smaller than M-JPEG files, so they can be transmitted over a narrower bandwidth. In CCTV applications, MPEG-4 allows a style of transmission where an “anchor” image is transmitted, and then another image is not transmitted until something in the image changes. This minimizes the number of images transmitted when there is no movement in a location. For this reason, MPEG-1 (and other frame-based codecs) can conceivably be perceived as a better source of forensic evidence since each frame or image is being sent as opposed to the updates. MPEG-4 offers a wide range of resolution sizes from 64 x 48 pixels to 4096 x 4096 pixels.

4-15.3.5 Following MJPEG, Wavelet is another frame-based compression codec that is commonly used. Wavelet operated in the 30Kbps to 7.5Mbps range and 8-30 frame rate speeds. Typical Wavelet resolution sizes are 160 x 120 pixels and 320 by 240 pixels.

4-15.4 With regard to bandwidth, there are two general system architecture factors:

4-15.4.1 On-site and hard-wired cameras

4-15.4.2 Off-site image transmission cameras.

4-15.5 Bandwidth is not as big an issue for on-site cameras because generally the cameras are hardwired (copper or fiber) and the distances are shorter. It is relatively easy to increase bandwidth by adding conductors. Off-site cameras, on the other hand, are more costly to add because the camera images have to be transmitted over conductors (typically leased) that cross property lines.

4-15.5.1 One technique for conserving bandwidth from off-site remote cameras to a Dispatch Center is to locate the DVR(s) at the remote facility. Information can be downloaded to a DVR local to the remote location at a high resolution and frame rate. If a video motion or other alarm event occurs (such as a door contact alarm), information can be transmitted to the Dispatch Center for review. This technique of only transmitting video images back to the Dispatch Center when an alarm occurs conserves bandwidth and relieves the Dispatch Center personnel of continually watching monitors.

4-15.5.2 Another advantage of placing the DVR at the remote site is that if communications are lost between the remote site and the Dispatch Center, camera image archives are still available at the DVR at the remote site. The downside to this configuration is that constant non-alarm camera images are not available at the Dispatch Center.

## 4-16 WHITE BALANCE

4-16.1 White balance is the ratio of black to white on a CCTV camera image. Most cameras (80%) are supplied with automatic white balance. Auto white balance ought to be used when the camera background image is changing. While it is possible to procure cameras with manual black-white balance, this should only be done in a very stable black-white image environment.

## 4-17 CCTV CAMERA EMPLOYMENT FOR INTRUSION DETECTION

4-17.1 **Background.** Originally, cameras were employed for intrusion detection by allowing an operator to continually view images on display screens. Intrusion detection occurred by human recognition of an intrusion event. Issues of operator fatigue, distractions and number of monitors that can be effectively observed left a lot of room for missing an intrusion event. While camera technology has not changed significantly in the last decade, the introduction of digital images and software programming capability has improved significantly. So while the camera housing, the lens, focal length and associated image are basically the same, the ability to digitally process the digital image in a manner that allows automated intrusion detection has seen a tremendous increase in technology in the last ten years. Programming trip wires can allow automated alarm notification with no prior human involvement. Methods for detecting intruders by CCTV systems include video motion detection, video content analysis, and motion path analysis.

4-17.2 **Video Motion Detection.** (VMD) makes use of software usually provided in the camera (or in the DVR) to analyze differences in contrast between the image pixels over time. If the contrast changes from one moment to the next, the associated software is capable of detecting the difference. Video Motion Detection was the industry’s first attempt to provide automated alarm notification on detecting motion. It was also initiated to reduce the tremendous storage requirements of CCTV information when closed circuit television systems converted to digital images. Reduced memory requirements were achieved because if there were no pixel changes, the system was programmed not to store video. This technique saved some hard disk drive space. The downside of Video Motion Detection is that it alerts on everything in a scene that moves (or causes pixel changes). This could be an object blowing across the field-of-view, snow falling, rain, waves on water, tree leaves moving or simple lighting changes as a cloud moves overhead. Initial Video Motion Detection systems experienced many false alarms or alarms of pixel changes that were not actual intrusion events.

4-17.3 **Video Content Analysis.** (VCA) or Artificial Intelligence (AI) was the next evolutionary step for CCTV system improvement for intrusion detection. Video Content Analysis (synonymous with Artificial Intelligence is sometimes referred to as “Smart Video: or “Intelligent Video”. Video Content Analysis classifies images within a camera’s field-of-view. Programming algorithms differentiate an animal from a person. The algorithms start by noticing pixel changes. Additional programming takes into account color changes, speed changes, types of motion, patterns within the motions, and degrees of freedom within each motion type. Video Content Analysis can filter out potential causes of nuisance alarms such as animal movement, rain, snow, birds, and so forth.

4-17.3.1 A variant of Video Content Analysis pertains to asset protection as opposed to intrusion detection. In this method, the camera focuses on a specific asset – such as a safe. As long as the camera continues to see the safe than no alarm signal is sent. Obscuration or removal of the safe can be programmed to generate an alarm signal.

4-17.4 **Motion Path Analysis** systems use complex computer algorithms to not only detect motion within a scene, but also to determine the rate and direction of motion. With these systems it is possible to identify things such as vehicles traveling the wrong direction on a one-way street, vehicles moving faster than allowable, and vehicles that stop moving. Motion path analysis has the ability of installing virtual trip wires with complex rules and can be programmed to differentiate between nuisances and targets. An example of this is vehicle within a site moving in a normal path of operational traffic (assume left to right) can be programmed as a normal event. Movement of a vehicle in the opposite direction (right to left in this case) can be programmed to generate an alarm for subsequent assessment and action. This technology may be suitable for PTZ or long-range thermal imaging systems. When motion is detected, the system zooms to the target and tracks it.

## 4-18 CCTV EQUIPMENT CONSIDERATIONS

4-18.1 Considerations when *designing* a CCTV system include:

4-18.1.1 Weather conditions such as fog, mist, rain, and snow. Obtain the environmental requirements such as maximum wind speed, high and low temperatures, as well as humidity information to aid in determining which equipment to use.

4-18.1.2 For work at an existing installation, determine if a new system or expansion of the existing system is best. Some of the factors to consider in weighing the cost of a new system versus modification/expansion to an existing system are as follows:

1. Determine the capacity of the existing system to accept new cameras.

2. Determine if the existing system is adequate in terms of adequate picture quality and technology.

3. Determine the cost savings associated with making use of existing equipment, especially an existing matrix switcher.

4. Determine if the new system or device is compatible with any existing devices such as cameras and matrix switches. Rewiring for new cameras and devices is labor-intensive and can be expensive.

4-18.1.3 Use proven technology. Dealers will try to sell the latest and greatest, which may or may not be proven technology.

4-18.1.4 Look for ease-of-use.

4-18.1.5 Cameras to be used in conjunction with infrared lighting (black and white cameras or dual mode cameras) should not have an infrared filter on the camera.

4-18.1.6 Specify whether or not auto-white balance or manual white balance shall be used. Normally auto white balance will be recommended. The exception would be an environment where there is a stable black-white image.

4-18.1.7 Coordinate with the lighting designer to provide appropriate light for both interior and exterior (site) cameras.

4-18.1.8 For interior cameras, ensure sufficient lighting is available to assess alarms at all hours of the day. Use strategically placed night-lights to ensure internal visibility at night.

4-18.1.9 For outside locations, specify tamper-resistant housings or other vandal-proof features for remote areas.

4-18.1.10 Investigate the scalability of the system. If more cameras are needed locally or remotely, can new systems be added with as little effort as possible?

4-18.1.11 Understand the service plan. Manufacturers provide service and maintenance programs. Some have premier service plans that provide feature upgrades and enhancements on computer-based video recorders.

4-18.1.12 Consider how the images will be viewed, the number of monitors needed to support the system, and how multiple camera scenes will be multiplexed onto a common monitor (not every camera requires an individual monitor).

4-18.1.13 Determine if the system operators need zoom and focus capability from their workstations.

4-18.1.14 Some camera installations may have difficult viewing conditions in terms of exposure to a variety of lighting conditions from morning fog, to afternoon direct glare, to evening shade or nighttime darkness. For these locations, ensure the camera has backlight compensation features (typically a gain or sensitivity setting on the camera). In rare cases, control of the backlight compensation setting may need to be made available back at the Dispatch Center. This is an additional control signal that is not often required, but could be a design requirement for specific cameras.

4-18.1.15 Specify auto-iris for outdoor applications and determine if interior lighting conditions change such that it should be specified for interior applications.

4-18.1.16 CCTV cameras should not be installed in areas that may compromise classified material (such as SCIFs) or where individuals expect a certain level of privacy:  restrooms, locker rooms, and private offices..

4-18.1.17 Ensure secure mounting for exterior cameras. Mount them on buildings or other rigid structures whenever possible. Although rarely needed, gyro-stabilized lenses are available for high vibration (high-wind) areas.

4-18.2 Considerations when *implementing* a CCTV system include:

4-18.2.1 The main concern with remote video monitoring is data security. Unless adequately protected, it may be possible for a hacker to gain access to remote video sites. To reduce the possibility of unauthorized access, user name and password protection is an important feature that must be implemented. A firewall and video encryption should also be employed to dramatically reduce the chance of unauthorized entry into the system.

4-18.2.2 Use ample light. The most common reason for poor quality images is that the light level is too low. Generally, the more light the better the images. With lighting levels too low, images become noisy and blurry with dull colors.

4-18.2.3 Scene illumination should be even across the field-of-view of the camera, with a target light-to-dark ratio of 4:1 and maximum light-to-dark ratio of 8 to 1 (marginally acceptable).

4-18.2.4 Avoid backlight. Try to avoid bright areas in the images. Bright images might become over-exposed (bright white) and objects might appear too dark. This problem typically occurs when one tries to capture an object in front of a window.

4-18.2.5 Reduce the contrast. A camera adjusts the exposure to obtain good average light level in the image. A person in front of a white wall tends to appear too dark. If a gray wall is used instead this problem does not exist.

4-18.2.6 Sensor size. The lens must make an image large enough for the sensor. The larger the sensor, the more expensive the lens. A lens made for one-half inch will work for one-half inch, one-third inch, and one-quarter inch sensors, but not for a two-thirds inch sensor. If a lens made for a smaller sensor is used on a bigger sensor the image will get black corners.

4-18.2.7 Focal length. Wide-angle lenses have a better depth of field than telephoto lenses. This means that you can focus both close to the camera as well as at a distance. Telephoto lenses require a more precise focus adjustment.

4-18.2.8 Iris. Always use auto-iris lenses for outdoor applications, as discussed in the *Outdoor Cameras* subsection and indoor applications as discussed in the *Indoor Cameras* subsection.

4-18.2.9 Ensure that the monitor viewing area in the Dispatch Center is free from glare and is ergonomically adjusted for viewing by response personnel.

4-18.2.10 Consider using video quad-processors versus video multiplexers to put multiple cameras on the same screen. This configuration eliminates choppy movements.

## 4-19 CCTV SYSTEMS DESIGN GUIDANCE

4-19.1 Table 4-5 provides additional design guidance and recommendations for designing CCTV systems.

**Table 4-5. CCTV Design Guidance and Recommendations**

| Issue | Recommendations |
|---|---|
| **Camera Angle of View and Placement** | If video motion detection will be used, the camera should aim perpendicular to the path of the adversary. This creates the greatest contrast and best sensitivity to video motion.<br>If video motion detection will not be used, and image recognition is desired (facial or license plate viewing), then aim camera directly at adversary path. |
| **Camera Type Recommendations**<br>**Fixed Cameras** | Fixed camera use is recommended for collecting data at specific risk areas. Risk area video shall capture the following:<br>- Record 100% of persons entering and leaving the risk area.<br>- Record 100% of activity within the risk area entry location. |
| **Camera Type Recommendations**<br>**PTZ Cameras** | PTZ camera use is recommended for allowing integrated camera call up with alarms and permit security to view activity in key areas of facility.<br>Camera call up integrates PTZ cameras to automatically be programmed to point to designated perimeter gates, building perimeter doors, loading dock doors and other critical areas if they are opened, and the video image(s) shall appear on designated security monitors. |
| **Environmental Considerations for Exterior Cameras** | All exterior cameras must have outdoor housing with integral heater and blower units. This shall include both pole-mounted cameras and exterior units mounted to buildings.<br>Weather tight conduit shall be used in exterior applications.<br>Any exterior camera that has a potential to receive a lightning strike shall utilize fiber optic cable with a video transceiver unit to optically isolate the video system head end from the field device to avoid damaging the primary CCTV controls equipment. |

| | |
|---|---|
| **Perimeter CCTV Recommendations** | Provide color PTZ cameras capable of viewing and recording the entire parking lot, entry and exit points, and normal walk paths.<br>Provide color PTZ cameras capable of viewing and recording all perimeter doors.<br>Provide color PTZ cameras capable of viewing exterior chemical storage, electrical substations, generators or other critical areas.<br>Provide fixed color cameras viewing and recording vehicle license plates as vehicles are driven onto property. |
| **Security Guard Monitor Considerations** | Security CCTV monitors should be evaluated based on the level of security personnel that will be viewing the images.<br>The minimum number of displays should be one.<br>A better configuration is two displays with one dedicated for alarm call-up and the scanning different cameras.<br>For complex systems, require custom configurations and evaluations.<br>The final configuration must take into account: (a) the number and frequency of simultaneous alarms, and (b) the number of facilities being monitored. |
| **Camera Frame Rate** | **Non-alarm mode:**<br>Poor: 1 fps<br>Recommended: 3 fps<br>Very Good: 5 fps.<br>**Alarm mode:**<br>Acceptable: 10 fps<br>Recommended: 15 fps<br>Very Good: 20 fps. |
| **Long Range Thermal Imagers** | Consider for critical perimeter and cases where detection in fog, rain, snow are important. Criticality of installation must justify premium price of the camera. |

| | |
|---|---|
| **CCTV Employed as IDS** | Video motion detection (motion-activated cameras) may work as fixed detectors in narrow spaces such as doors and hallways.<br>For exterior, wide-area surveillance, video content analyis/motion path analysis is recommended over video motion detection to cut down on the number of nuisance alarms. |
| **CCTV Encoding/Decoding (Codec) Schemes** | Only use standard codec schemes – do not use proprietary schemes.<br>Use frame-based codec schemes when forensic evidence may be required. |

# CHAPTER 5

# INTRUSION DETECTION SYSTEM

## 5-1 OVERVIEW

5-1.1 The function of an IDS is to detect intruders. The detection of an intruder starts the “clock” on the Detect, Delay, Respond timeline addressed in Chapter Two, Electronic Security Systems Overview. The principal elements of an IDS include interior sensors, exterior sensors, IDS CPU or local controllers, communications and interfaces with ACS, CCTV and the Dispatch Center. These elements, and others that comprise an IDS, are shown in Figure 5-1 (shown on next page). An IDS requires integration with a process and mechanisms and for assessing and responding to intrusion alarms.

## 5-2 CENTRAL PROCESSING UNIT (CPU)

5-2.1 The key for any IDS is that it be accurate, timely, and allow for assessment and verification of alarm conditions. Therefore, it is important that the CPU allow for integration to the ACS, CCTV system and provide a user interface to allow security personnel to interact with alarm events.

5-2.2 On a comprehensive system, the CPU of the IDS may include a computer workstation and printer. The CPU analyzes alarm information from the sensors, and provides output information to the ACS, CCTV system and computer workstation. The IDS CPU and the ACS CPU may be integrated into a single controller. This typically occurs when the IDS inputs are principally simple digital inputs. When more complex sensors (typically exterior sensors) are used, either local controllers or a separate IDS CPU will be required as shown in Figure 5-2.

5-2.3 A specialized case of an IDS CPU occurs in a SCIF. In this situation, the Premise Control Unit (PCU) receives signals from all associated sensors in the SCIF’s alarm zone and establishes the alarm status. The alarm status is immediately transmitted to the Monitoring Station. Within the Monitoring Station, a dedicated alarm-monitoring panel (or central processor) monitors incoming PCU signals. On receiving an alarm signal, a Monitoring Station’s enunciator generates an audible and visual alarm for the monitoring personnel.

## 5-3 INTERIOR SENSORS

5-3.1 This section covers both interior point sensors and interior volumetric sensors. For additional information on interior IDS sensors to include types, purposes, principles of operation, common causes of false alarms, and appropriate applications refer to DoD 0-2000.12.H.

**Figure 5-1. Example Intrusion Detection System (IDS)**

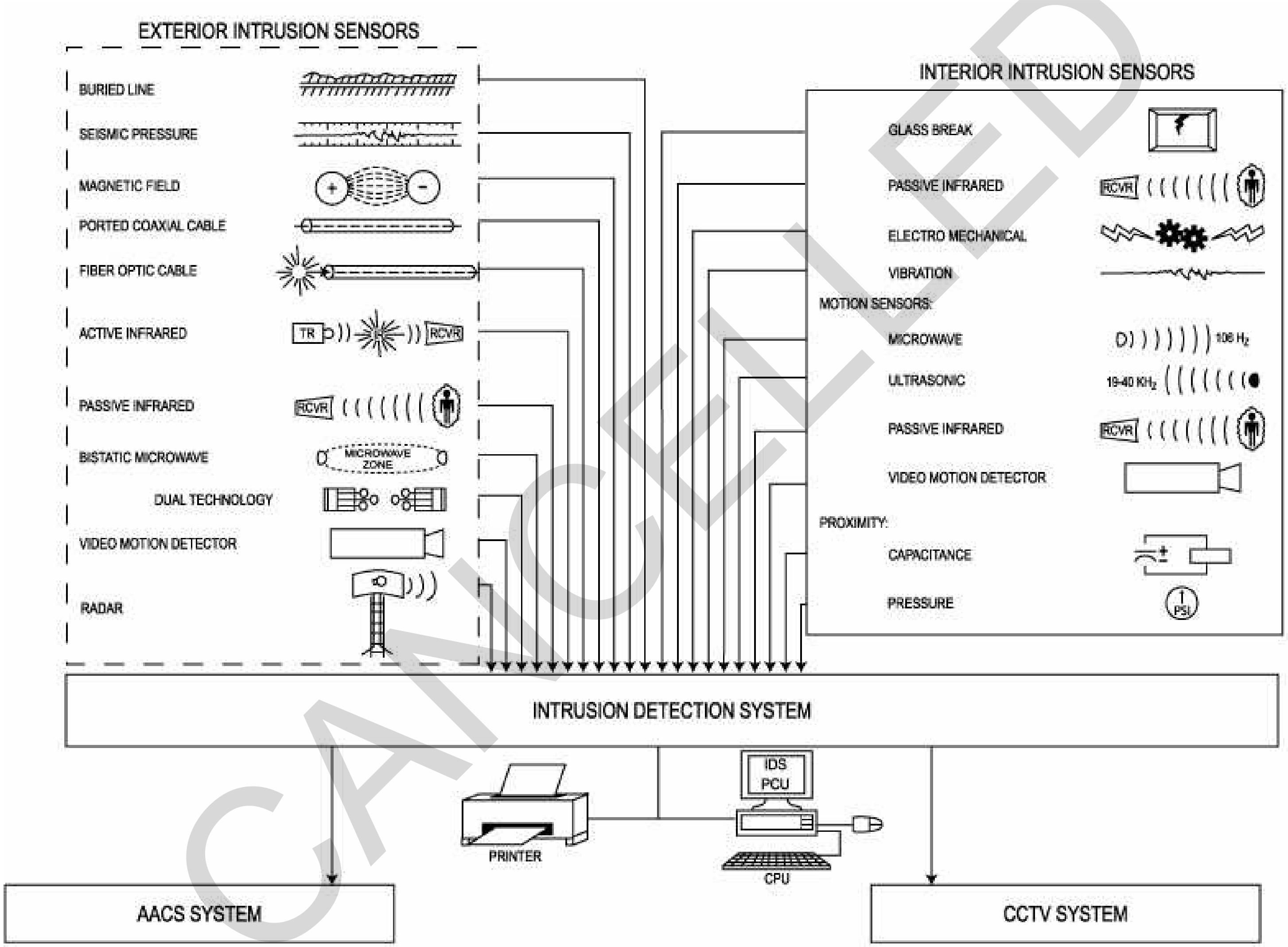
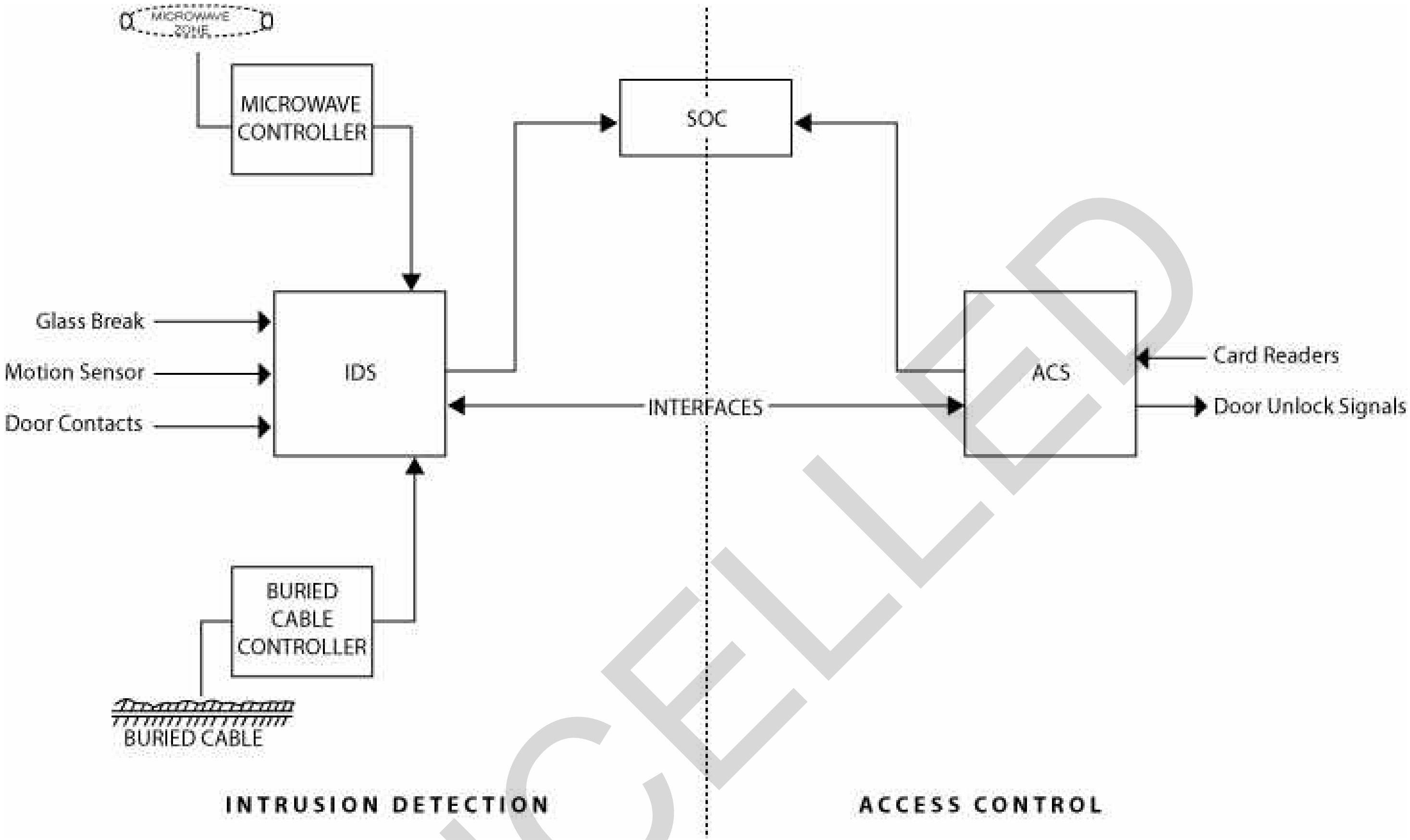


**Figure 5-2. Separate ACS and IDS CPUs**



### 5-3.2 Interior Point Sensors

5-3.2.1 **Balanced Magnetic Switch(s) (BMS).** BMS use a magnetic field or mechanical contact to determine if an alarm signal is initiated (for example, if an access portal such as a door, window, or roof hatch is been opened). BMS differ from standard magnetic status switches in that BMS incorporate two aligned magnets with an associated reed switch. If an external magnet is applied to the switch area, it upsets the balanced magnetic field such that an alarm signal is received*.* Standard magnetic switches can be defeated by holding a magnet near the switch. Mechanical contacts can be defeated by holding the contact in the closed closed position with a piece of metal or taping them closed. Balanced magnetic switches are not susceptible to external magnetic fields and will generate an alarm if tampering occurs. Therefore, only specify balanced magnetic switches for access portal sensors. Figures 5-3, 5-4, and 5-5 show some typical applications of BMS.

Figure 5-3. Sample Door Configuration

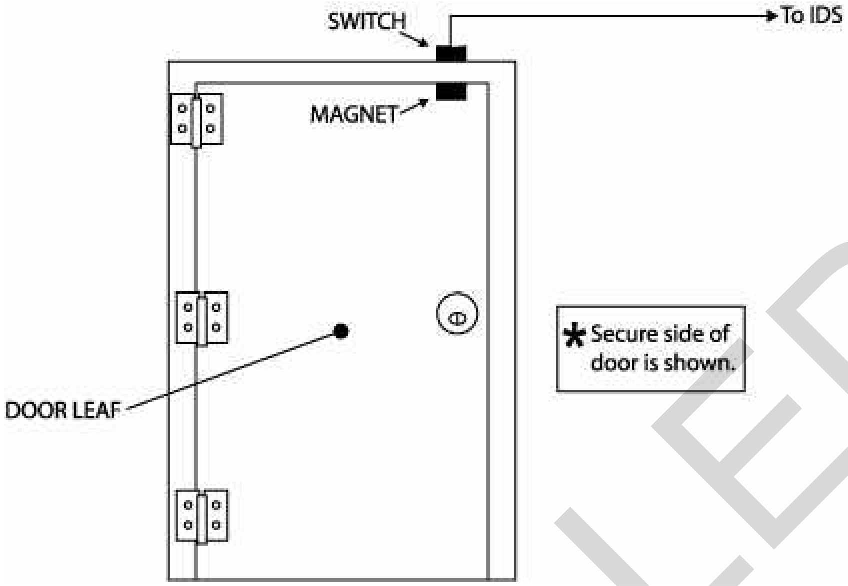


Figure 5-4. Sample Window Configuration

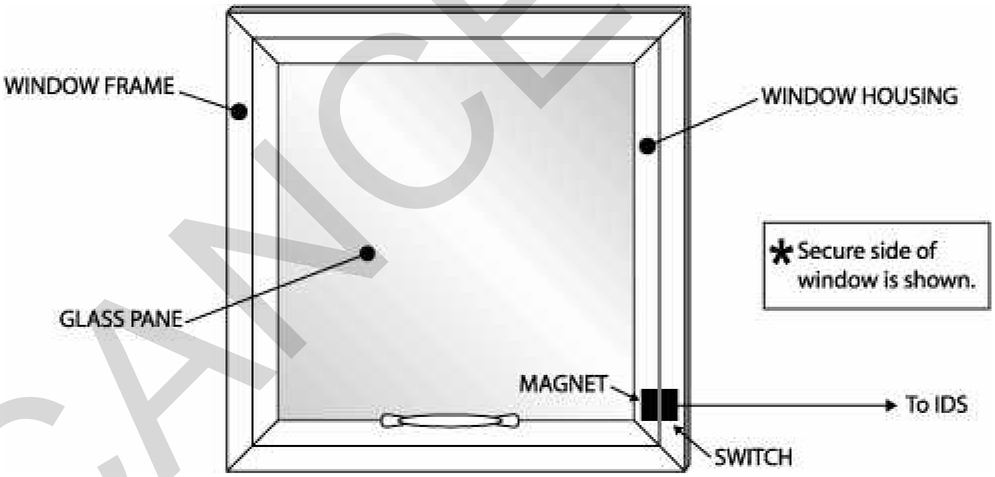
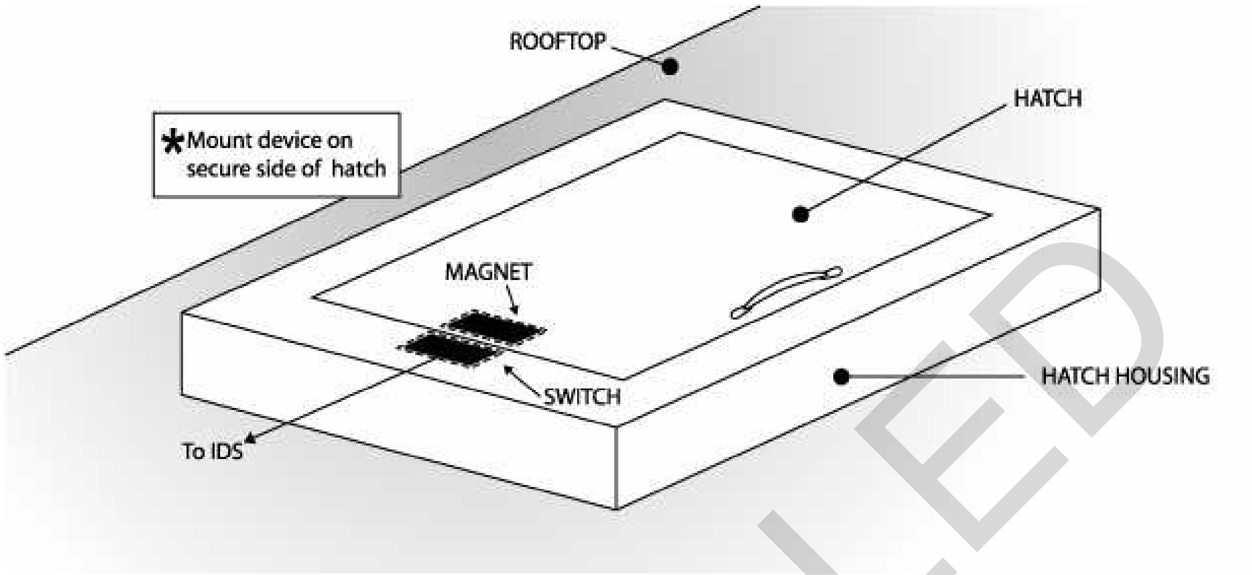


**Figure 5-5. Sample Roof Hatch Configuration**



5-3.2.2 **Glass Break**. Glass break sensors are a good intrusion detection device for buildings with a lot of glass (windows, doors with glass panes). Glass as an exterior protection barrier is easily defeated. Windows can be quickly and easily broken. Consider the case of installing a card reader on an administrative exterior door. The determined intruder will not let the door lock deter the intrusion effort, but can take the option of breaking nearby accessible windows.

5-3.2.2.1 There are three basic types of glass-break sensors: acoustic sensors (listens for an acoustic sound wave that matches the frequency of broken glass), shock sensors (feels the shock wave when glass is broken), and dual-technology sensors (senses acoustic and shock vibrations). Glass-break sensors should be used in conjunction with other methods (such as volumetric sensors) because they do not sense motion or intrusion from entering a door or hatch.

5-3.2.2.2 Glass break sensors can be used to cover several windows.

5-3.2.3 **Glass Types**. There are a variety of glass types: plate, tempered, laminated, and wired. For inhabited facilities, UFC 4-010-01 requires laminated glass for windows. Most glass break sensors work with all glass types to include laminated glass.

5-3.2.4 Glass Break Sensor Guidance:

5-3.2.4.1 Do not use window mounted glass break sensors.

5-3.2.4.2 Glass break sensors should only be used in protected areas with windows on the ground floor or that are easily accessible.

5-3.2.5 Use volumetric sensors in conjunction with glass break sensors in protected areas.

5-3.2.6 Use dual-technology glass break sensors (acoustic and shock wave). There is not a significant price difference between a simple acoustic sensor and a combination sensors (acoustic and shock). For the nominal component price increase, which is a fraction of the total installed cost, the increased capability justifies the higher cost.

5-3.2.7 Check glass break sensor specifications to ensure they are rated for the type of glass used, typically laminated glass.

5-3.3 **Motion Activated Cameras**. A fixed camera with a video motion feature can be used as an interior intrusion point sensor. In this application, the camera can be directed at an entry portal (door) and send an alarm signal when an intruder enters the field-of-view. This device has the added advantage of providing a video image of the event. The key to good video motion detection is contrast. Activation of a door will provide sufficient contrast. An intruder in a white lab coat walking down a corridor with white walls might not generate sufficient contrast. Application of video motion cameras as an interior intrusion device requires coordination with the building architect and or interior designer. Interior video motion cameras can also be alarmed by someone cutting off the lights. As with any camera, the better the lighting, the better the detection capability. Use of cameras, requires careful consideration of the background image and normal or abnormal changes to that background image.

Internal motion-activated cameras act as a detection means for stay-behind covert intruders.

5-3.4 **Other CCTV Detection Methodologies.** (Refer to Chapter 4 for subsections on video content analysis and motion path analysis in the section *Employment of CCTV Cameras for Intrusion Detection*.) When these other methodologies are used, consider the following guidance:

5-3.4.1 Require good lighting.

5-3.4.2 Best done where there is a stable background image and intrusion would generate sharp image contrast.

5-3.5 **Interior Volumetric Sensors**. Volumetric sensors monitor an internal area to detect the presence of an intruder. There are several types of volumetric sensors including acoustic, infrared linear beam sensors, passive infrared (PIR), ultrasonic and dual-technology (microwave and PIR). The most commonly used are dual-technology sensors.

5-3.6 **Acoustic Sensors.** Acoustic sensors use passive listening devices to monitor building spaces. An application is an administrative building that is normally only occupied in daylight working hours. Typically, the acoustic sensing system is tied into a password protected building entry control system, which is monitored by an off-site Central Station. When someone has logged into the building with a proper password, the acoustic sensors are disabled. When the building is secured and unoccupied, the acoustic sensors are activated. After hours intruders make noise which is picked up by the acoustic array and an alarm signal is generated.

5-3.6.1 Acoustic sensors act as a detection means for stay-behind covert intruders.

5-3.7 **Passive Infrared (PIR) Sensors** are one of the most common interior volumetric intrusion detection sensors. PIRs pickup heat signatures (infrared emissions) from intruders by comparing infrared receptions to typical background infrared levels. Typically, activation differentials are 3 degrees Fahrenheit. These devices work best in a stable environmentally-controlled space**.**

5-3.7.1 Different cones or cowlings can be placed on the PIR to focus or spread-out the coverage of the detection window. In other words, standard supplied covers for lens can be made to provide a more narrow or wider sensor coverage area.

5-3.7.2 While not a security application, PIRs are often used as an automatic request to exit device for magnetically locked doors. In this application, the PIR acts as the automatic sensor for detecting an approaching person in the exit direction for magnetically locked doors.

5-3.7.3 PIR Sensor Guidance:

5-3.7.4 Do not use near exterior doors where the sensor can be exposed to sudden changes in background environmental temperature.

5-3.7.5 Best use is in interior climate-controlled spaces.

5-3.7.6 PIRs can receive false alarms from other heat radiating objects such as heat-system registers, rodents, pets, or other warm objects (in one case a mop bucket with hot water in it).

5-3.7.7 PIRs can also be defeated by a trained, slow-moving intruder. (Very hard to achieve.)

5-3.7.8 PIRs are much more sensitive to travel crossing its sensing area as opposed to travel toward the sensor.

5-3.8 **Ultrasonic Sensors** use active transmission of sound waves to pick up intruders much like a radar transmitter and receiver. To get an alarm signal, a signal must be transmitted, bounced off an intruder and receipt signal received. Ultrasonic sensors are rarely used.

5-3.9 **Dual-technology sensors** use both microwave and PIR sensor circuitry within one housing. An alarm condition is generated if *either* the microwave or PIR sensor detects an intruder. In some dual-technology sensors, alarm settings may be adjusted to require that both the microwave and the PIR unit detect an intruder presence before an alarm condition is generated. Since two independent means of detection are involved, false alarm rates are reduced when configured in the "AND" condition (both microwave and PIR sense an intruder). Dual-technology sensors can only be used in a SCIF, vault, or secure room if the technologies operate in an "OR" configuration (either the microwave or PIR sense an intruder). Therefore dual technology sensors are not recommended for this application.

5-3.9.1 Dual-technology sensors act as a detection means for stay-behind covert intruders. Table 5-1 provides application notes for interior IDS sensors.

**Table 5-1. Application Notes – Interior IDS Sensors**

| Application | Sensor Type | Notes |
|---|---|---|
| **Doors** | Balance magnetic switch (BMS). | Proper alignment and properly installed doors minimize false alarms.<br>Used in conjunction with volumetric sensors. |
| **Windows** | BMS<br>Break Glass Sensor<br>Acoustic<br>Shock<br>Dual Technology | Use combination acoustic/shock wave sensor.<br>Used in conjunction with volumetric sensors. |
| **Roof Hatches** | BMS | Proper alignment and proper installation minimize false alarms.<br>Used in conjunction with volumetric sensors. |
| **Room/Hallways** | Volumetric Sensors:<br>Passive Infrared<br>Microwave<br>Dual Tech (PIR & MW)<br>Ultrasonice. | Do not use dual-tech devices in SCIFs. |
| **Walls** | Vibration Sensors<br>Fiber Optic Sensors. | Design to detect a compromise of a wall to a secure area. |

## 5-4 EXTERIOR SENSORS

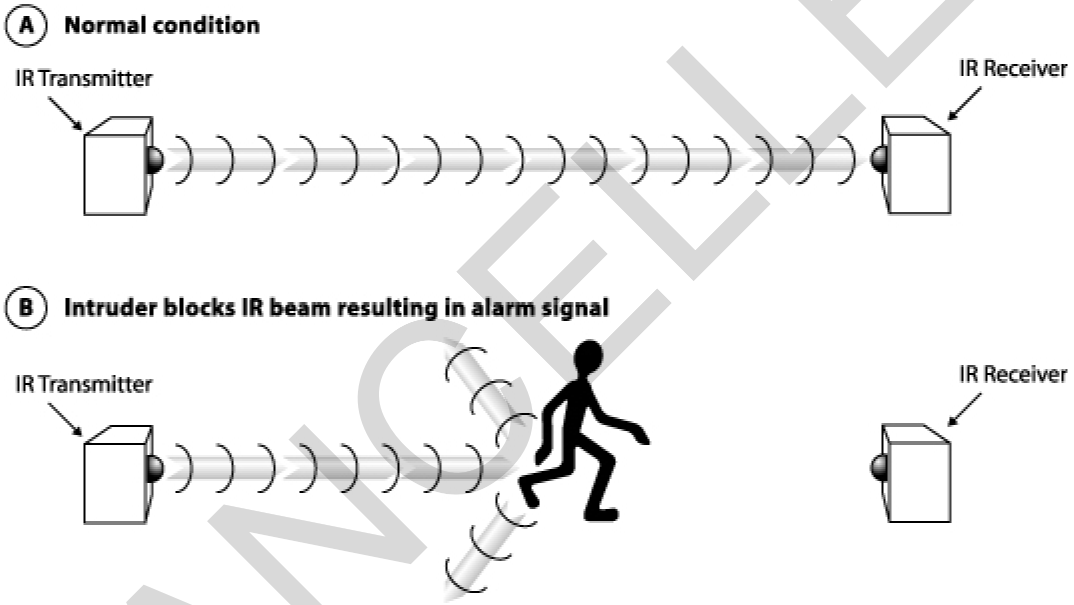
5-4.1 This section covers exterior sensors for intrusion detection in the following categories: (1) open terrain sensors such as infrared and microwave sensors, (2) property/fence-line sensors such as electro-mechanical systems and fiber-optic sensing systems, and finally (3) other sensor technologies such as buried cable and wide area sensors.

5-4.2 **Open Terrain.** Open terrain sensors include infrared, microwave systems, combination (dual technology), vibration sensors and new emerging video content analysis and motion path analysis (CCTV) systems. In general, open terrain sensors work best on flat, cleared areas. Heavily or irregular contoured areas are not conducive to open terrain sensing systems.

5-4.2.1 **Infrared.** Passive sensors can work well in exterior environments, but outside interference issues of reflected light or radiated light have to be considered.

5-4.2.2 **Active.** Active infrared sensors transmit an infrared signal via a transmitter. The location for reception is at a receiver**.** Interruption of the normal IR signal indicates an intruder or object has blocked the path. The beam can be narrow in focus, but should be projected over a cleared path. Refer to Figure 5-6 for a conceptual diagram of how an active infrared IDS works.

**Figure 5-6. Active Infrared IDS**



Infrared Sensor Guidance:

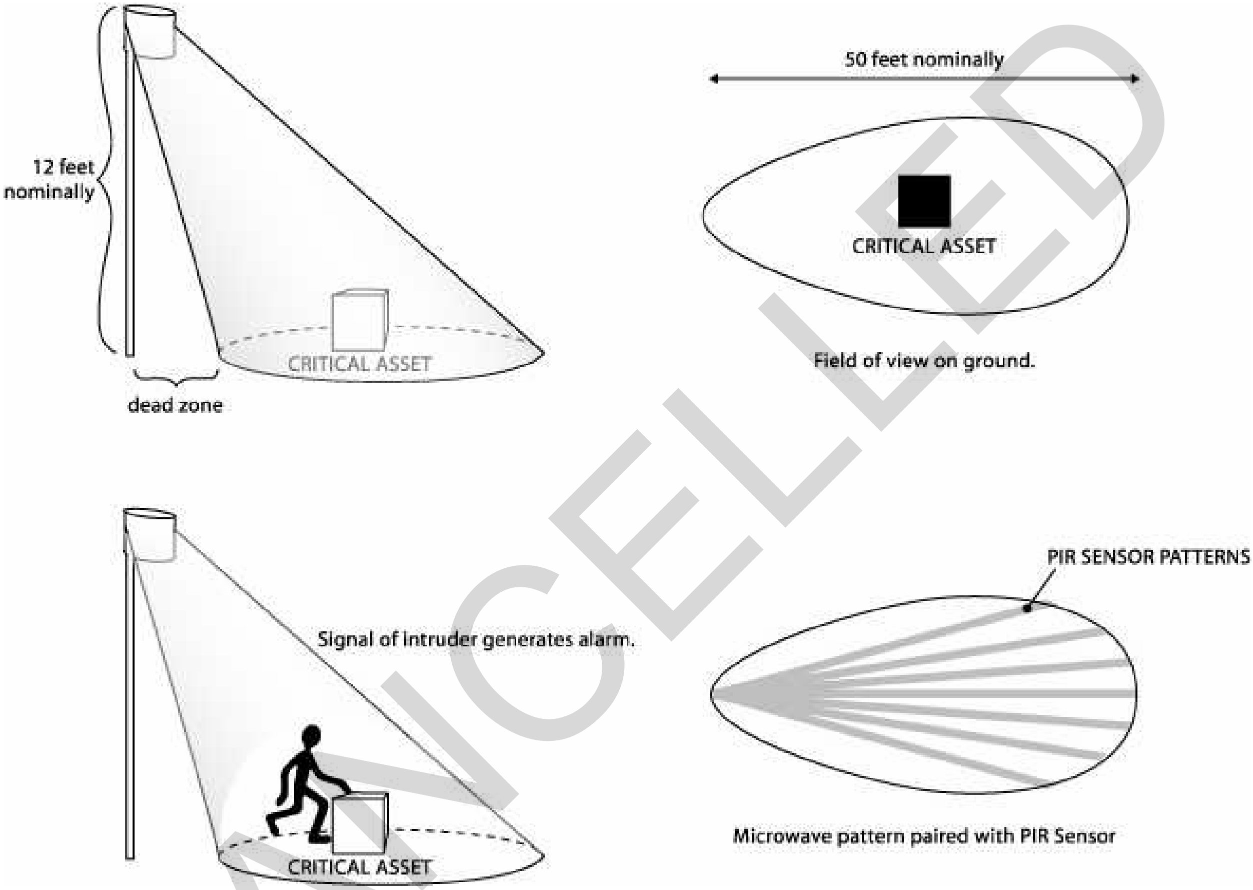
5-4.2.3 Check that the terrain is suitable for clear signal transmission.

5-4.2.4 Infrared arrays do not work well in areas with heavy snowfall because drifts or snowmounds cover sensors and or block transmission and reception paths.

5-4.3 **Microwave sensors** come in two configurations: bistatic and monostatic. With both bistatic and monostatic sensors, the sensors operate by radiating a controlled pattern of microwave energy into the protected area. The transmitted microwave signal is received, and a base level “no intrusion” signal level is established. Motion by an intruder causes the received signal to be altered, setting off an alarm. Microwave signals pass through concrete and steel and must be applied with care if roadways or adjacent buildings are near the area of coverage. Otherwise nuisance alarms may occur due to reflected microwave patterns.

5-4.3.1 **Monostatic**. Monostatic microwave sensors use a single sensing unit that incorporates both transmitting and receiving functions. Many monostatic microwave sensors feature a cut-off circuit, which allows the sensor to be tuned to only cover within a selected region. This helps to reduce nuisance alarms. Refer to Figure 5-7 for illustrations of a monostatic microwave sensor and associated footprints.

**Figure 5-7. Monostatic Microwave Sensor and Associated Footprints**



5-4.3.2 **Bi-static**. Bi-static microwave sensors are more commonly used than monostatic sensors for wide-area surveillance. Bi-static microwave sensors use a transmitter and receiver pair**.** Bi-static sensors work over longer distances than mono-static sensors. Typical distances for transmitter-receiver pairs are ten to six hundred feet for X-band frequencies and one hundred to fifteen hundred feet for Y-band frequencies. The bi-static transmitter typically sends out a high frequency open-band radio frequency in a 3-8 degree pattern. (Common microwave frequencies are X-band 10 GHz or Y-band 24 GHz.) Refer to Figure 5-8 and Figure 5-9 (next page) for illustrations of bistatic microwave sensor operation.

5-4.3.3 **Microwave Design Guidance and Recommendations**

5-4.3.3.1 The detection zone should be free of bushes and obstructions.

5-4.3.3.2 The detection zone should be graded to within three inches to detect crawling intruders.

5-4.3.3.3 Grass should be kept cut to less than three inches. A gravel surface prepared for water drainage is better than a grass surface. Since a typical microwave pattern is ten feet by ten feet, a twenty-foot wide gravel bed works well.

5-4.3.3.4 Avoid water puddles. The wave action of wind on water can cause nuisance alarms.

5-4.3.3.5 For high security applications, consider use of stacked sensors (one sensor on top of another), with the lower frequency (wider/broader pattern) on top and the higher frequency (more focused pattern) to detect crawling intruders on the bottom.

5-4.3.3.6 Do not place sensors too close to perimeter fences. Wind action on the fence fabric can cause false alarms.

**Figure 5-8. Bistatic Microwave Sensor Operation**

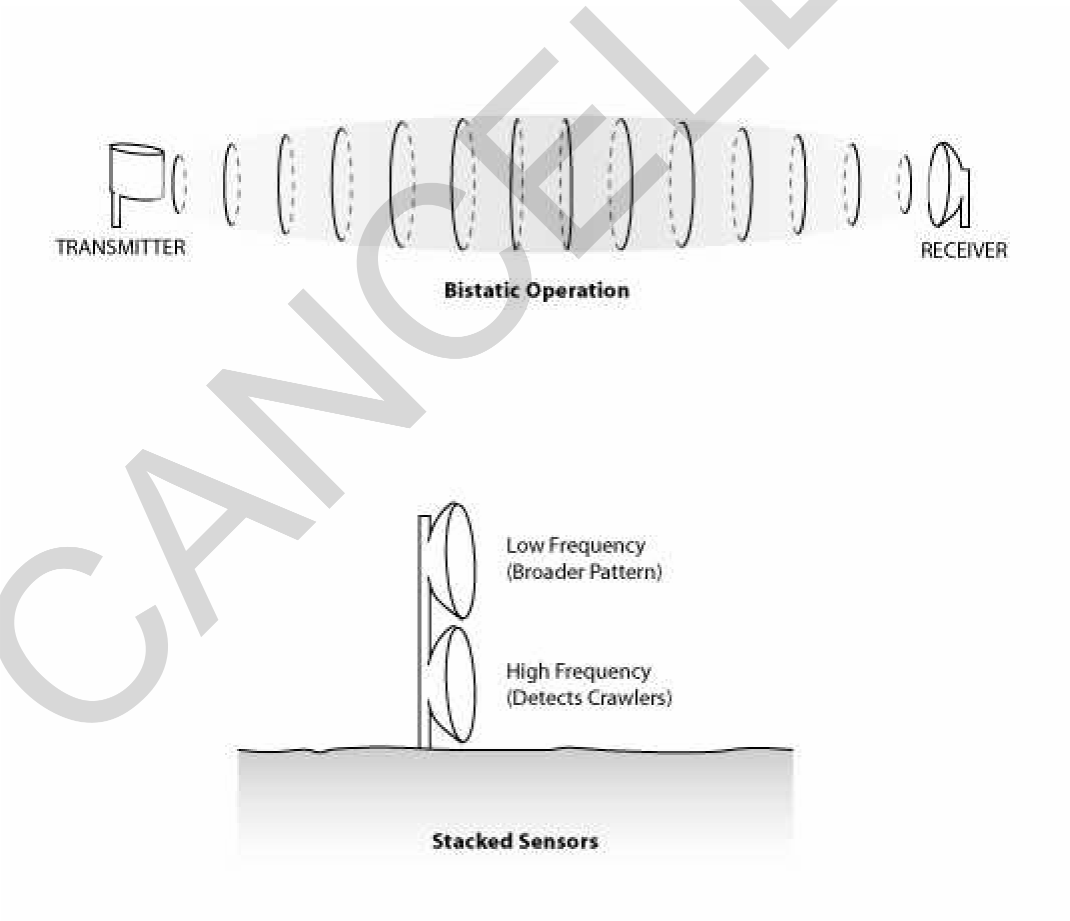
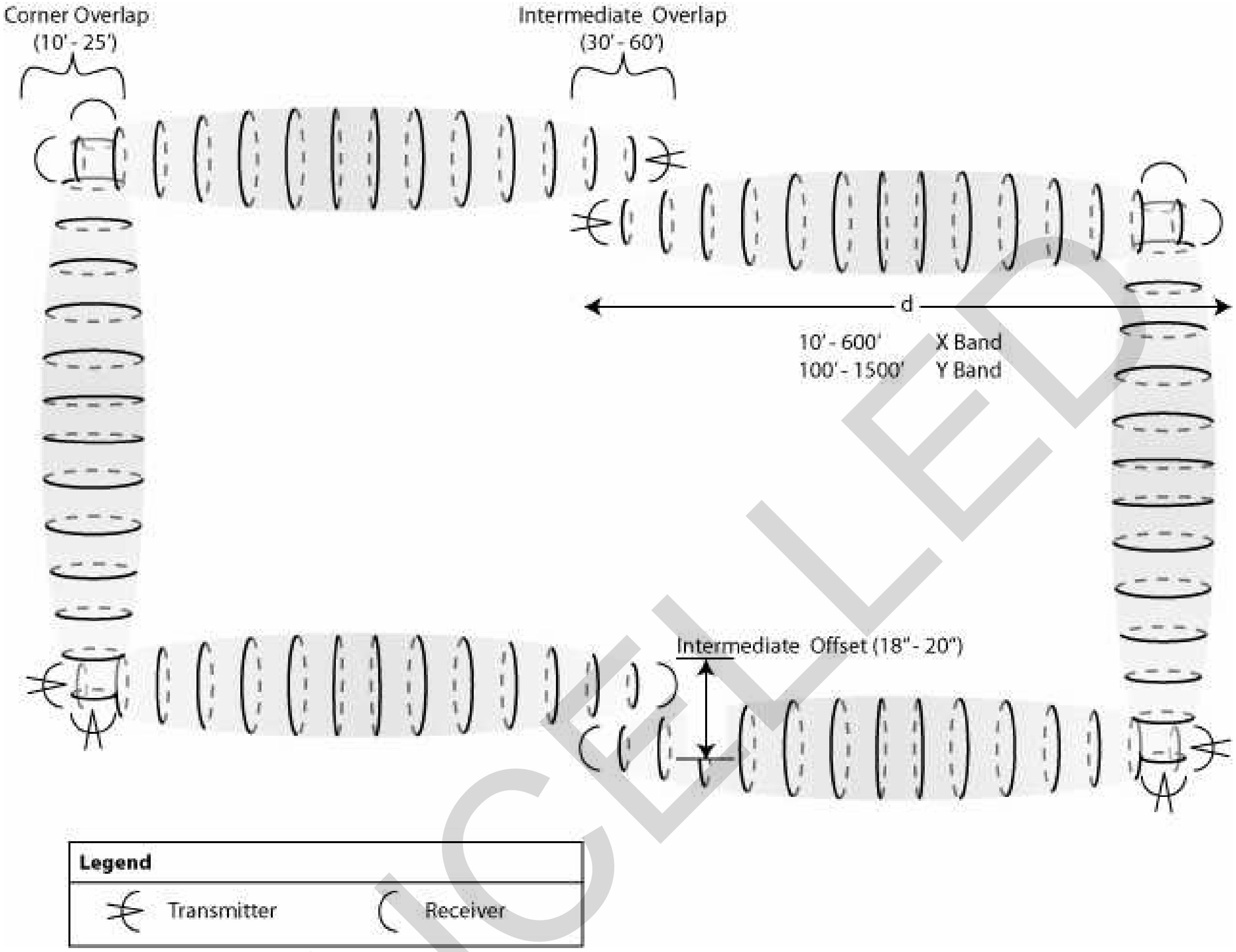


Figure 5-9. Typical Bistatic Microwave Layout and Guidance



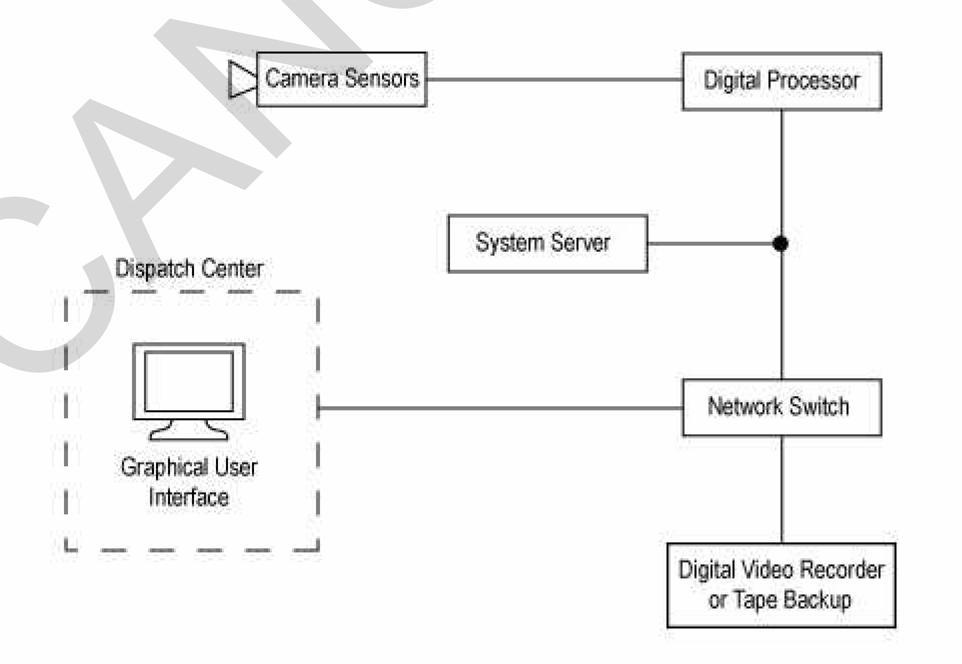
5-4.3.4 **Combination.** As discussed previously, dual-technology sensors use a combination of PIR and microwave technology. Techniques of "ANDing" or "ORing" the microwave signal and the PIR signal are reviewed in Paragraph 5-5.

5-4.3.5 **Vibration sensors** sense intrusion through vibrations caused by personnel or vehicular movement. These sensors are not well employed near railroad tracks, roadways, rock quarries, or runways. Many of these systems use wireless battery-powered sensors to send alarm signals to a notification station.

5-4.3.6 **Video Content Analysis and Motion Path Analysis**. The newest intrusion detection technology for intrusion detection is sophisticated software analysis of the camera images such as video content analysis and motion path analysis. As previously discussed in Chapter Four, CCTV camera systems are increasingly being used as intrusion detection systems. Application of complex algorithms to digital CCTV camera images allow CCTV systems to detect intruders. The software programming (algorithms) start by detecting pixel changes and evolve to include filtering to differentiate and filter out normal video events (leaves blowing, snow falling) from alarm events (intrusion). The application of software rules can further evolve to differentiate between a cat walking across a parking lot (irrelevant) to a person trespassing through the parking lot (relevant to an alarm event). The application of complex software algorithms to CCTV digital images takes on the aspect of artificial camera, whereby the camera and processors become “smart video” and start to emulate a human operator. The differences between a smart camera and a human operator are principally twofold. It takes a lot of complex software programming (and associated rules) to get the camera systems ability to differentiate and assess video events as well as the human mind. With more and more project applications, the gap is closing as the camera systems come closer to emulating the capabilities of fully alert, very motivated, intelligent security guard fresh into a watch shift. The advantage of Video Content Analysis and Motion Path Analysis is that the camera systems do not get tired. Studies have demonstrated that after twenty minutes, the ability of a guard to discern an abnormal event are severely degraded. Video content analysis systems do not suffer fatigue and remain “alert” after monitoring hundreds of video events in a watch shift. Video content analysis systems can monitor more cameras, more effectively, with less operators at a reduced total cost (less dispatch center/command center staff) – hence, the increase in popularity of their application. Figure 5-10 displays a typical system architecture for a video content analysis system.

5-4.3.6.1 In the current marketplace, video content analysis and motion path analysis are supported by software companies which are different from the traditional CCTV component/system suppliers. These software companies supply unique digital processing hardware and write software to process the digital image information. At the writing of this guide, the cost of video content analysis varies from $2500 to $5000 per camera on top of the installed cost of the camera.

**Figure 5-10 Video Intrusion Detection System**



5-4.3.6.2 Table 5-2 provides additional design guidance and recommendations of use of video content analysis and motion path analysis systems for wide area intrusion detection.

**Table 5-2. Video IDS Design Guidance and Recommendations**

| Issue | Recommendations |
|---|---|
| **Camera Type** | Use fixed cameras for video content analysis.<br>Consider use of pan-tilt-zoom cameras for assessment, once intrusion detection occurs. |
| **Image Resolution** | 320 by 240 minimum. |
| **Frame Rate** | 15 frames per second minimum. |
| **Camera Mounting** | 35-40 feet; higher is better.<br>Cameras mounted at 8-10 feet offer the ground end up with too much occlusion.<br>Camera must be stable with good physical support. |
| **Distance Between Cameras** | 200-300 feet. |
| **Orientation to Fenceline or Perimeter** | Parallel to the fence line or down to 45 degrees to the fenceline. (It is easier to detect an intruder moving laterally than pick up a target traveling down the throat of a sensor/camera axis.) |

5-4.4 **Property/Fence Line Detection.** Several types of fence-mounted perimeter IDS exist. With all fence-mounted systems it is critical that the fence construction be of high quality, with no loose fabric, flexing, or sagging material. The fence should also have solid foundations for posts and gates. Otherwise nuisance alarms may occur. Five types of exterior fence-sensing systems will be discussed: (1) electro-mechanical systems, (2) taut-wire systems, (3) coaxial strain-sensitive cable, (4) Time Domain Reflectometry (TDR) systems, and (5) fiber-optic strain-sensitive cable systems.

5-4.4.1 **Electro-mechanical systems.** According to the *Perimeter Security Sensor Technologies Handbook,* electro-mechanical fence-sensing systems use either mechanical inertia switches or mercury switches to detect a fence climbing or cutting incident. An electronic controller looks for momentary contact openings of the inertia or mercury switches. For more information on electro-mechanical fence-sensing systems refer to the *Perimeter Security Sensor Technologies Handbook.* Due to advances with other (better) technologies, electro-mechanical systems are not recommended for DoD use.

5-4.4.2 **Taut wire systems.** Taut-wire fence-sensing systems use a series of parallel wires under tension with a numerous micro-switches attached to it. The system is very sensitive, but requires frequent maintenance. For more information on taut-wire systems refer to *The Design and Evaluation of Physical Protection Systems.*

5-4.4.3 **Coaxial strain-sensitive cable** systems use a coaxial cable woven through the fabric of the fence. The coaxial cable transmits an electric field. As the cable moves due to strain on the fence fabric caused by climbing or cutting, changes in the electric field are detected within the cable, and an alarm condition occurs**.**

Coaxial strain-sensing systems are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. Some coaxial cable systems are susceptible to electromagnetic interference and radio frequency interference.

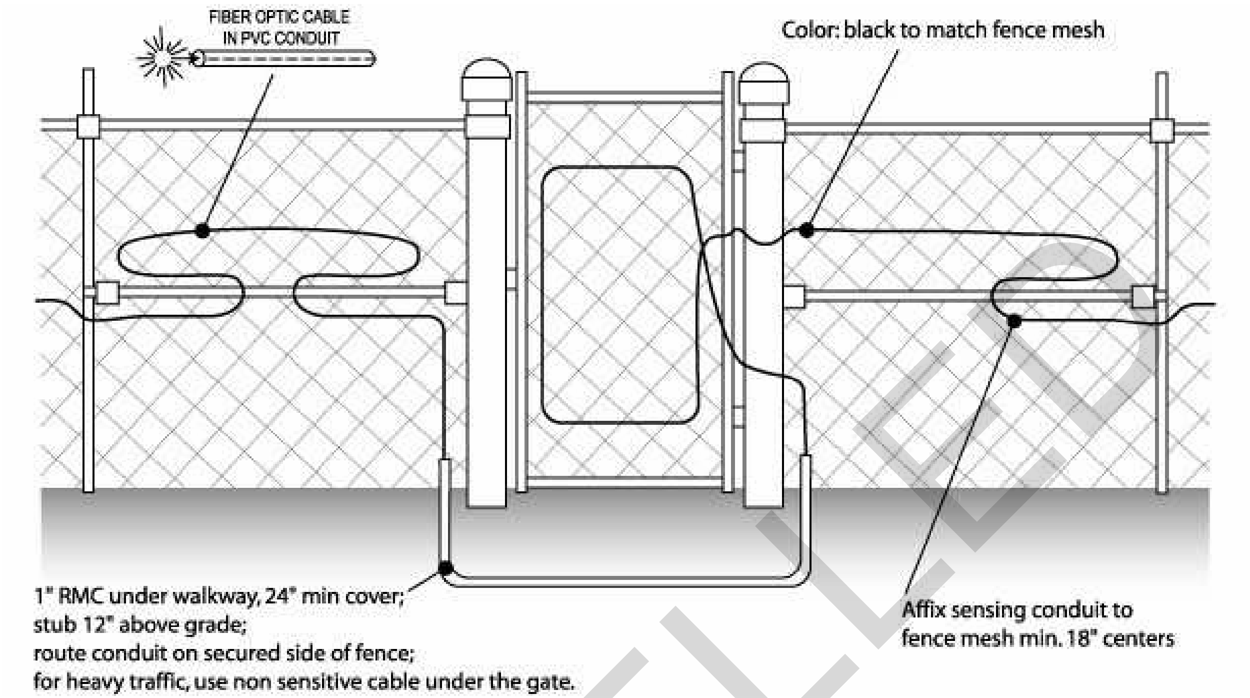
5-4.4.4 **TDR Systems.** Time Domain Reflectometry systems send an induced radio-frequency (RF) signal down a cable attached to the fence fabric. Intruders climbing or flexing a fence create a signal path flaw that can be converted to an alarm signal. When the conductor cable is bent of flexed, a part of the signal returns to the origination point. This reflected signal can be converted to an intrusion point by computing the time it takes for the signal to travel to the intrusion point and return. The cable can be provided in armored cable, which requires more than a bolt cutter to sever the sensing cable. These systems require their own processor unit and can be configured in a closed loop, such that if the cable is cut, a detection can be detected by the other return path.

5-4.4.5 **Fiber-optic** strain-sensitive cable systems are similar to the coaxial strain-sensitive cable systems. The fiber-optic system uses a fiber-optic cable, rather than a coaxial cable, woven through the fence fabric. Strain on the fence fabric causes micro-bending of the fiber cable, which is monitored by the control panel and generates an alarm condition. Figure 5-11 shows a typical fiber-optic fence detection illustration. Fiber-optic strain-sensing systems are relatively newer detection systems but have a strong following. The systems are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. The systems are impervious to lightning, electromagnetic interference, radio frequency interference, or other electronic signals and can be used over long distances.

5-4.4.6 **Defeat Measures and False Positives.** Possible defeat measures include tunneling, jumping, or bridging across the fence system. Careful climbing at corner posts may not generate sufficient vibration to generate an alarm condition.

Possible false positives can occur from debris, animals, and plants.

**Figure 5-11. Typical Fiber Optic Fence Detection System**


FIBER OPTIC CABLE
IN PVC CONDUIT
Color: black to match fence mesh
1" RMC under walkway, 24" min cover;
stub 12" above grade;
route conduit on secured side of fence;
for heavy traffic, use non sensitive cable under the gate.
Affix sensing conduit to
fence mesh min. 18" centers

## 5-4.5 Other Exterior Sensors

5-4.5.1 **Buried Cable** There are two common types: buried ported cable and buried fiber-optic cable. The two principle advantages of buried cable are that (a) it is covert, and (b) it follows the terrain. A limitation is buried cable systems do not work well with shrubbery or trees on it and require landscaping and maintenance. It is important that the cable be buried to a uniform depth. Changes in soil conductivity can effect the sensor readings.

5-4.5.2 **Ported Cable.** Ported cable comes in two principal configurations, Single cable and paired cable. A single cable system uses one cable to create a sensing field approximately 6 feet in diameter around the cable. Paired cable systems use two cables routed in parallel one to two feet apart. One cable transmits and the other receives a signal to create the sensing field.

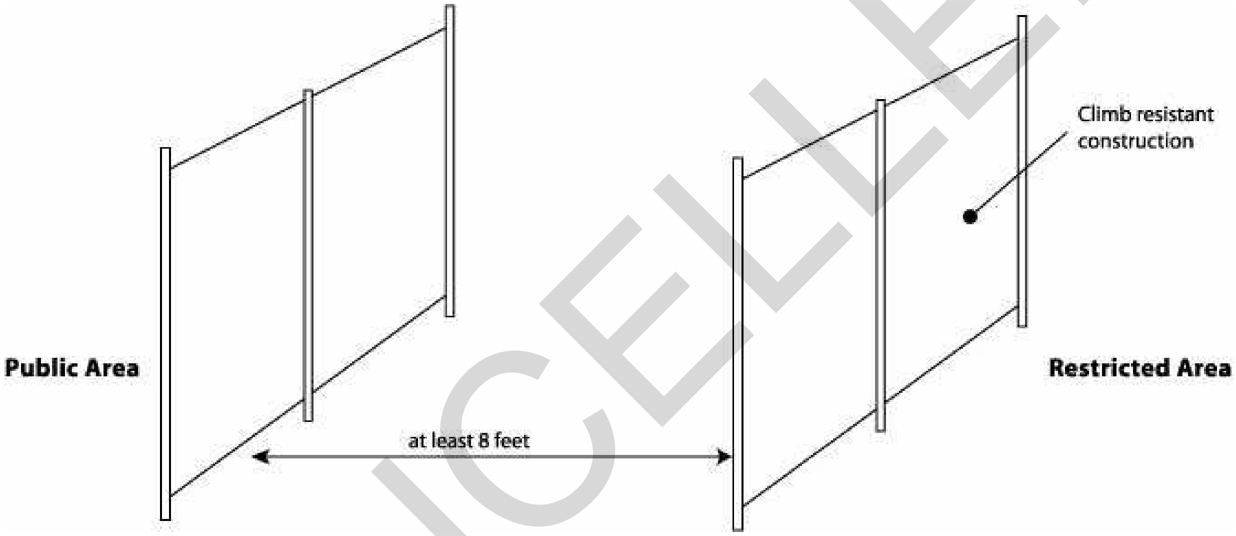
5-4.5.3 **Fiber Optic.** Fiber optic lines can be used to monitor pipelines or manholes.

5-4.5.4 **Wide Area Sensors:** Wide area sensors such as radar can be employed on logical approach paths for large terrain or water territories/boundaries. Wide area sensors can assist response forces with early alerting or tracking of intruders. This technology approach has the advantage of being able to detect intruders beyond the defined perimeter. In other words, the system can detect intruders before they have crossed the protected area's perimeter.

5-4.6 **False Alarm Causes for Exterior Sensors**. Table 5-3 displays typical false alarm causes for exterior IDS sensors. Snowfall, removal of snow, winds, temperature change, and rain drainage are some factors to consider in exterior sensor selection. Refer to the Perimeter Security Sensor Technologies Handbook for more information on exterior IDS sensors.

When fence detection sensors are used, the best application is to use a double-fence concept. In addition to adding an additional delay factor, the outer fence acts as an animal deterrent, while the detection system is best applied to the inner fence. Typically the fence should be a climb-resistant fence at least eight feet high with a minimum of eight feet of distance between the inner and outer fence, as shown in Figure 5-12. Use of concrete footings down to one foot below the surface helps limit mitigation by shallow tunneling.

**Figure 5-12. Fence Example**



### Table 5-3. False Alarm Causes—Exterior IDS Sensors

| Sensor Type | False Alarm Cause | Notes |
|---|---|---|
| **Active Infrared** | Animals<br>Wind-blown debris | Fencing mitigates animal false alarms |
| **Passive Infrared (PIR)** | Reflected light<br>Radiated heat | Not recommended |
| **Microwave** | Nearby movement outside IDS area | Use of dual-technology PIR minimizes false alarms |
| **Dual Technology** | Same as PIR and microwave | Good choice. Uses both microwave and PIR |
| **Vibration** | Railroads—trains<br>Roadways—vehicles<br>Runways—airplanes<br>Rock quarries—explosions<br>Seismic event | Only works well in low background vibration areas |
| **Coaxial Strain-Sensitive** | Wind flexing fence<br>EMI | Temperamental |
| **Fiber-Optic** | Improper noise level adjustment<br>Animal activity | Recommended technology, provided suitable fence-mount is provided and animals are excluded from the area |
| **Buried Cable** | Ground shifting due to standing or puddling water, or erosion. | Varying terrain or material composition (asphalt pavement to grass to gravel) requires adjusting sensitivity to match each material |
| **Ported Cable** | EMI<br>Movement of nearby vehicles or medium to large animals<br>Congregation of small animals. | Very susceptible to EMI from large electrical equipment or substations and should not be used near these installations |
| **Video Content Analysis**<br>**Motion Path Analysis** | Camera vibration.<br>Normal operational personnel/vehicular movement.<br>Lightning flashes. | Good camera mounting mitigates camera vibration issues.<br>Advanced programming can filter out false alarms from animals, rain, snow, birds, waves and so forth.<br>Video content analysis works best in a relatively stable video environment. For example, video content analysis works better in a flat desert environment than a volatile meteorological such as windy, rainy or foggy location. |

## 5-5 SYSTEM CONFIGURATION

5-5.1 Subcomponents of an IDS can be configured in an “AND” or “OR” configuration. In the “AND” configuration, two or more sensors must detect intrusion for an alarm notification to occur. In the “OR” configuration, only a single sensor need go into alarm for a notification to occur. The “AND” configuration is used when a concern about nuisance alarms exists. The “OR” configuration is more secure and is used to increase the probability of detection. An example is pairing two microwave sensor fields. In the “AND” configuration, both Field A and Field B have to be in alarm to cause alarm notification. In the “OR” configuration, if either Field A or Field B go into alarm, then an alarm signal is sent to the Dispatch Center. Addressable sensors allow the capability to switch the “AND/OR” configuration from the Dispatch Center. However for some facilities, such as SCIFs, this feature should be disabled. Table 5-4 displays the advantages and disadvantages of each configuration.

**Table 5-4. Advantages and Disadvantages of “AND” and “OR” Configurations**

| | Pros | Cons |
|---|---|---|
| **AND** | Decreased nuisance alarms | Decreased probability of detection |
| **OR** | Increased probability of detection | Increased nuisance alarms |

## 5-6 IDS DESIGN GUIDANCE

5-6.1 The IDS Designer must first determine the design objectives for the project, usually expressed as a Probability of Detection (Pd). Some sample requirements are a Pd of 95% for most assets and a Pd of 99% for critical assets. Understanding the requirement, the designer can then go about laying out the ESS and strategy. Consider a case study of having to provide a Pd of 99% for a critical asset. Some sample vendor-specifications for three types of IDS sensors are shown in Table 5-5.

**Table 5-5. Sample Probability of Detection Factors**

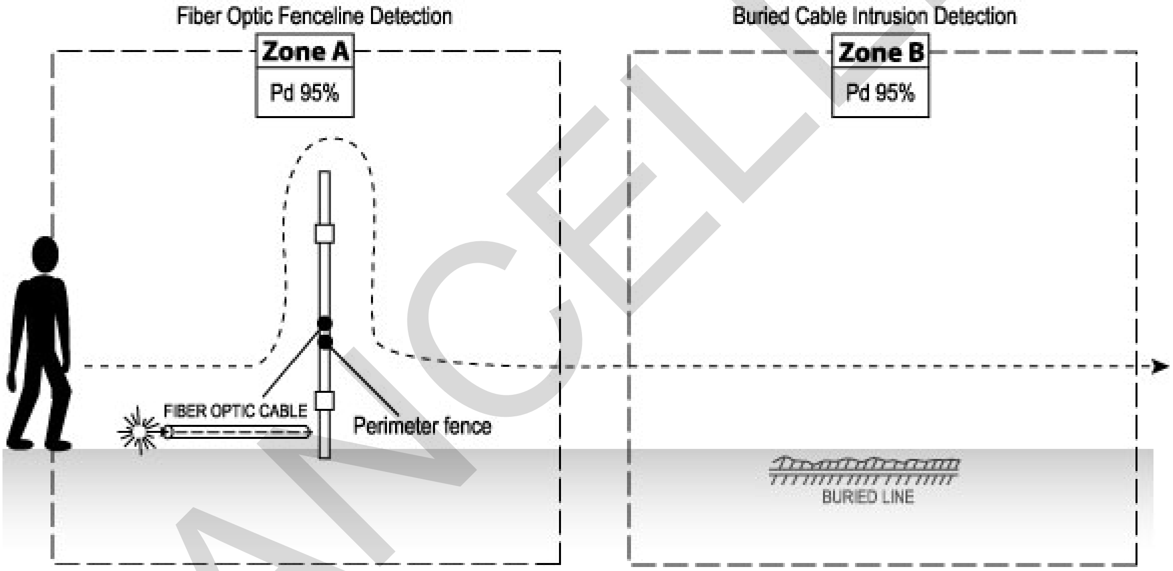
| Product | Probability of Detection |
|---|---|
| **Buried Cable** | 95% |
| **Fence-Mounted Fiber Optic** | 95% |
| **Microwave** | 99% |

5-6.2 For the purpose of demonstrating the application of different approaches, two alternatives for meeting the project requirement are presented. While an individual component probability of detection may not meet a more demanding specification, layering or combining components can result in a higher overall system probability of detection as illustrated below:

5-6.2.1 Option A: Use a microwave perimeter system with a Pd of 99%. The equipment and system meets the project objectives and no other IDS methods are technically required to meet the specified intrusion detection range.

5-6.2.2 Option B: If the scenario is such that terrain contour makes microwave technology unfeasible, the IDS designer could consider a zoned approach of combining a fence mounted fiber-optic detection system with a buried cable detection system as shown in Figure 5-13.

**Figure 5-13. Zoned Detection System**



5-6.3 If the two detection systems shown in Figure 5-13 are integrated in an electrical “OR” logic, an alarm from either system results in an IDS alarm. The resultant net Pd can be calculated as follows:

(Pd)A = 95%; therefore the probability of not being detected is (1-Pd)= 1-0.95= 5%

The probability of not being detected in Zone B is similarly calculated as 5% as well.

5-6.4 The net probability of not being detected by either Zone A or Zone B can be calculated by multiplying the chances of not being detected in either A or B together as follows:

= (1-Pd) A * (1-Pd) B

=5% * 5%

=0.25%

=0.0025.

Thus the probability of not being detected by either intrusion system A or B is 0.25%, which is another way of saying the probability of being detected is 99.75% or nominally 99%.

5-6.5 In the above example, two solutions of meeting a requirement to meet the Pd of 99% were analyzed. There are other options than the two discussed. The example presented is an academic case study to demonstrate different values of Pd for and methods of layered protection. It is based on convenient Pd factors for two common intrusion detection technologies based (fiber optic fenceline and buried cable). For each project, the IDS designer will have to design a solution taking into account project requirements, available technology, site-specific information, and possible causes of false alarms.

5-6.6 Additional IDS design guidance is provided in Tables 5-6 and 5-7.

**Table 5-6. IDS Design Guidance**

| Issue | Recommendations |
|---|---|
| **Door Status Monitoring** | Restricted area perimeter monitoring should be included at all building entrance and exit points, to include perimeter doors, roof hatch openings, and doors used for emergency egress.<br>Doors for emergency egress should include an audible device (door screamer) on the secured side.<br>All door monitoring should be via balance magnetic switches. The status switch contacts shall be closed when the door is closed. |
| **Redundant Path for Alarms** | In large critical systems, plan an alternate path for alarms. One method of achieving this is to route IDS alarms into the ACS and out to the Dispatch Center as an alternate path to a normal primary route of having the IDS inputs report directly to the Dispatch Centers. |

**Table 5-7 Exterior IDS Applications Table**

| Application | Sensor Type | Notes |
|---|---|---|
| **Fence line** | Taut wire | Very sensitive, high maintenance. |
| | Coaxial strain-sensitive | Works, susceptible to EMI. |
| | TDR | When fence is not in good condition.. |
| | Fiber Optic | More expensive, but better filtering. |
| | CCTV (Video Content Analysis/Motion Path Analysis) | Best current technology, can account for trees blowing or normal motion, but is the most expensive. |
| **Gates** | BMS | Simplest device, provide lightning protection. |
| | Fence detection systems. | Will detect a fence intruder that climbs the gate. |
| | Magnetic loop sensor | Will detect vehicles only. |
| | CCTV (Video Content Analysis/Motion Path Analysis) | Best current technology, can account for trees blowing or normal motion, but is the most expensive. |
| **Open areas** | Microwave | Works well in desert environments, does not work well around trees and un-cleared line-of-sight areas. |
| | Ported Coaxial | Does not work well near electrical substations, certain geographic areas with unusual magnetic influences. Can be effective, when used as part of a double-fence system. |
| | CCTV (Video Content Analysis/Motion Path Analysis) | Best current technology, can account for trees blowing or normal motion, but is the most expensive. |

*Note: Table 5-7 is not all inclusive of all exterior sensor options. Refer to text above for more detail*.

## 5-7 SUMMARY

5-7.1 In general, intrusion detection is challenging. There is no one single sensor system that works in all applications. Realistically, the best Pd that can be achieved by a single system is 95%. Given enough time and resources, all intrusion detection systems can be defeated. For simple installations with lower security needs, a fiber-optic fence-perimeter detection-system works well. For higher security applications, double fences/intermediate, gravel bed and microwave sensors offer improved security. Video content analysis is an up-and-coming technology that will only improve with time as software algorithms more closely simulate alert human operators.

# CHAPTER 6

# DATA TRANSMISSION MEDIA (DTM)

## 6-1 INTRODUCTION

A critical element in an integrated ESS is the data transmission media (DTM) that transmits information from sensors, access 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, and back to the Dispatch Center. An effective DTM link ensures rapid and reliable transmission of data, is resistant to compromise, has redundancy, and is conducive to rapid fault detection and repair.  A number of technology issues are relevant to implementing the DTM, such as bandwidth analysis, secure communications, network topology, communication redundancy, transmission modes or protocols, and transmission media. These issues are discussed in the following sections.

## 6-2 BANDWIDTH ANALYSIS

6-2.1 With any data-intensive transmission network, such as an electronic security system network, it is important to determine the amount of bandwidth consumed by the system under normal and alarm conditions. This can affect network cost, reliability, and transmission speed. An example bandwidth analysis is shown below in Table 6-1. For the DTM, design a system capable of handling the total bandwidth (plus contingency) for each link required in the system.

**Table 6-1. Example Bandwidth Calculations**

| Link | Facilities | Cameras in Alarm | Alarm Bandwidth (3.07 Mbps per Camera) | Cameras in Normal | Normal Bandwidth (0.61 Mbps per Camera) | Total Bandwidth (Mbps) |
|---|---|---|---|---|---|---|
| B-A | Building B to Command Center | 1 | 3.07 | 4 | 2.68 | 5.75 |
| C-A | Building C to Command Center | 1 | 3.1 | 9 | 5.5 | 8.6 |
| D-A | Building D to Command Center | 0 | 0 | 0 | 0 | 0 |
| E-A | Building E to Command Center | 2 | 6.1 | 10 | 6.1 | 12.2 |
| F-A | Building F to Command Center | 0 | 0 | 0 | 0 | 0 |
| G-A | Building G to Command Center | 2 | 6.1 | 10 | 6.1 | 12.2 |
| H-A | Building H to Command Center | 0 | 0 | 0 | 0 | 0 |
| I-A | Building I to Command Center | 1 | 3.1 | 1 | 0.6 | 3.7 |
| J-A | Building J to Command Center | 2 | 6.1 | 22 | 13.4 | 19.6 |
| | | | | | | |

*Note: The assumptions in the table above are based on 640 by 480 pixels resolution, a 20:1 compression ratio, and 10 frames rate per second (frame rate speed) in alarm and 2 frames per second in the non-alarm mode. Refer for Chapter 4 for bandwidth calculations.*

## 6-3 SECURE COMMUNICATIONS

6-3.1 No matter what transmission mode or media is selected, it is important that a method for securing communications be included. This includes physical protection, such as providing rigid metallic conduit for all conductors, as well as electronic protection, such as encrypting communication transmissions. Refer to the Chapter Nine for the subsection on Tamper Protection, which includes a discussion on physical protection of conductors as well as more general information on encryption requirements.

## 6-4 NETWORK TOPOGRAPHY

6-4.1 One of the initial steps in designing and evaluating a security DTM is to identify the topology to be used. Additionally, the designer should coordinate network requirements with installation security and the communications office. Typically, networked security systems are typically a Proprietary Security Network. Refer to Chapter 8, “ESS Subsystem Integration” for more information.

6-4.2 Three general network topographies are possible: star, ring, and fully meshed. The concepts apply to intra-site system architectures as well as inter-site regional configurations. A brief description of each topography follows.

6-4.2.1 **Star.** The star, or “hub and spoke” network involves a central Dispatch Station (or head-end) and single communication lines out to individual sites (or field panels).

The disadvantage to a star topography is that if one of the links is disabled or severed then communication is lost to that node. The unconnected node may still well operate through distributed intelligence, but will be unable to receive updates from the rest of the system. For example, if a new credential holder were added to the access list this information could be downloaded to a remote site or panel from a central location. With a severed link, these updates are not available unless the information were uploaded at the local site/panel. Conversely, if a credential holder were deleted from the access database, a "severed" site/panel would continue to allow access until communications were re-established or a local upload made. Figure 6-1 shows a star topography for both an inter-site architecture and an intra-site architecture.

6-4.2.2 **Ring.** The ring topography communicates through a loop. This topography is slightly more robust than a star topography that in the event of failed link, communications can sill be maintained through the "backside" direction on the loop. Communications may be a slower in this backup mode of operation, but would be sustainable. Figure 6-2 shows a ring topography for both the inter-site and intra-site scenario.

6-4.2.3 **Fully Meshed.** The most robust topography is a fully meshed topography depicted in Figure 6-3. This topography has backup means of communication, such that if any one link is disabled or severed, communications have an alternate path to communicate directly between nodes. This is the preferred ESS network topography.

**Figure 6-1 Star Topographies**

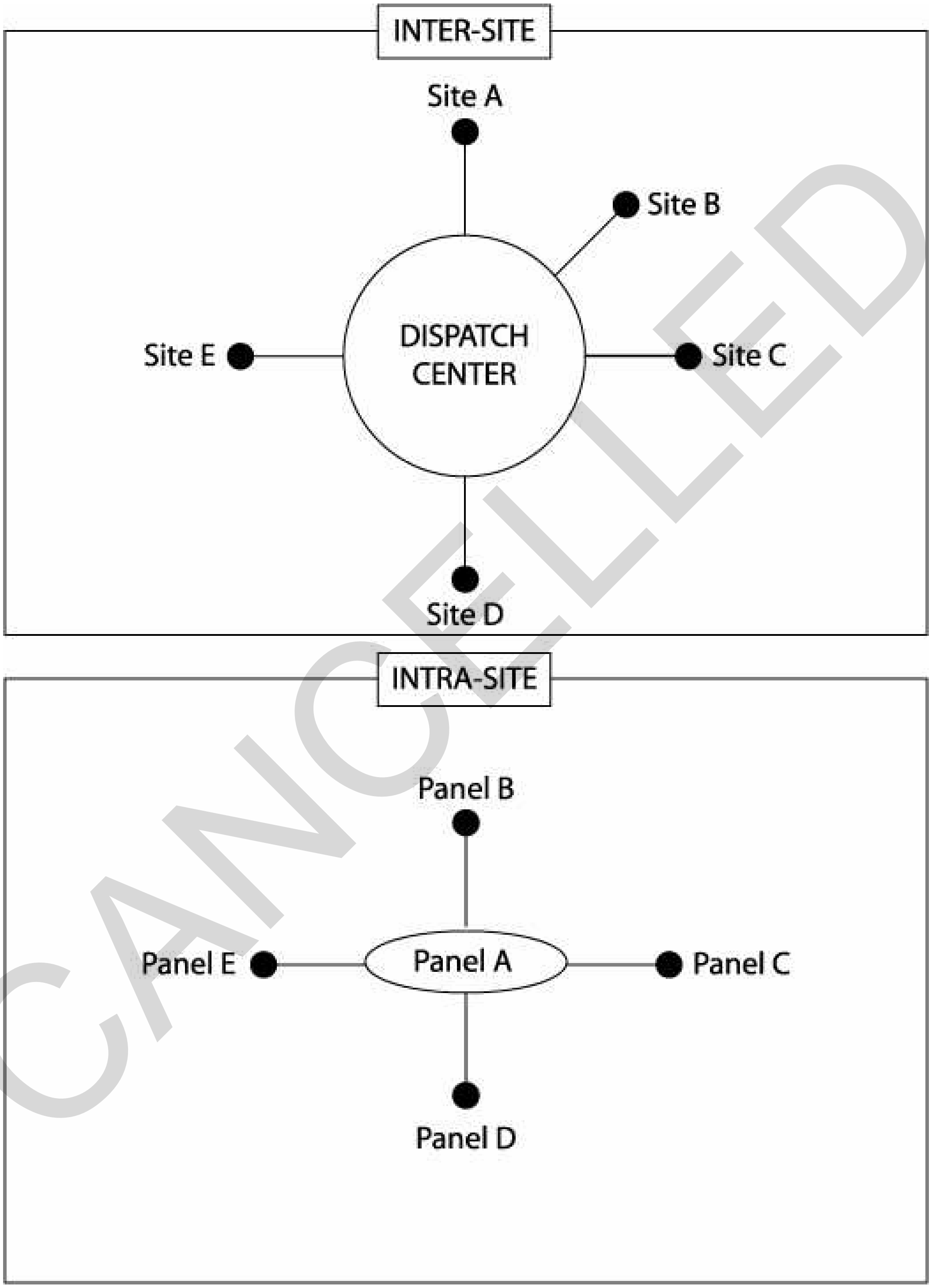


**Figure 6-2. Ring Topographies**

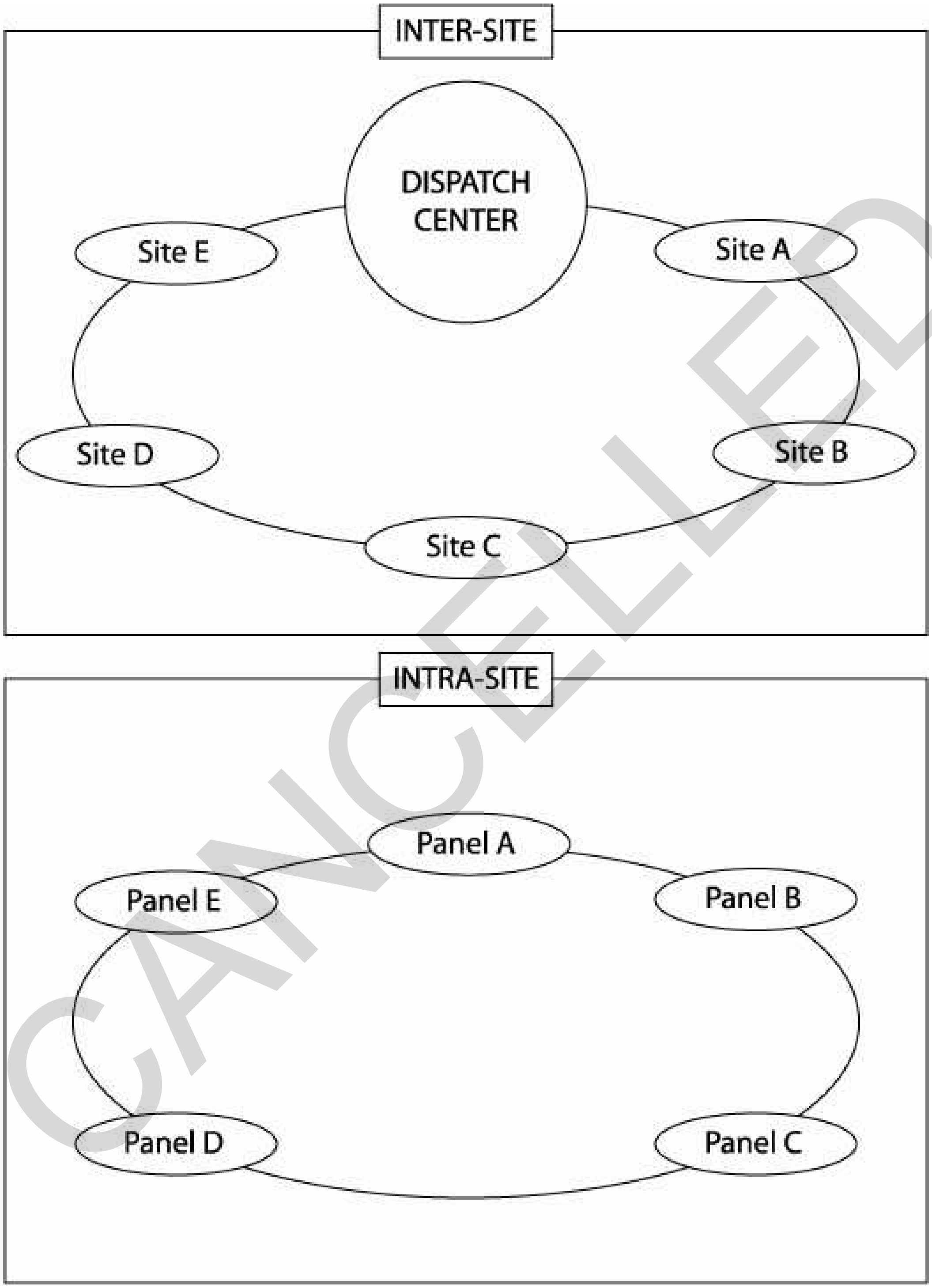
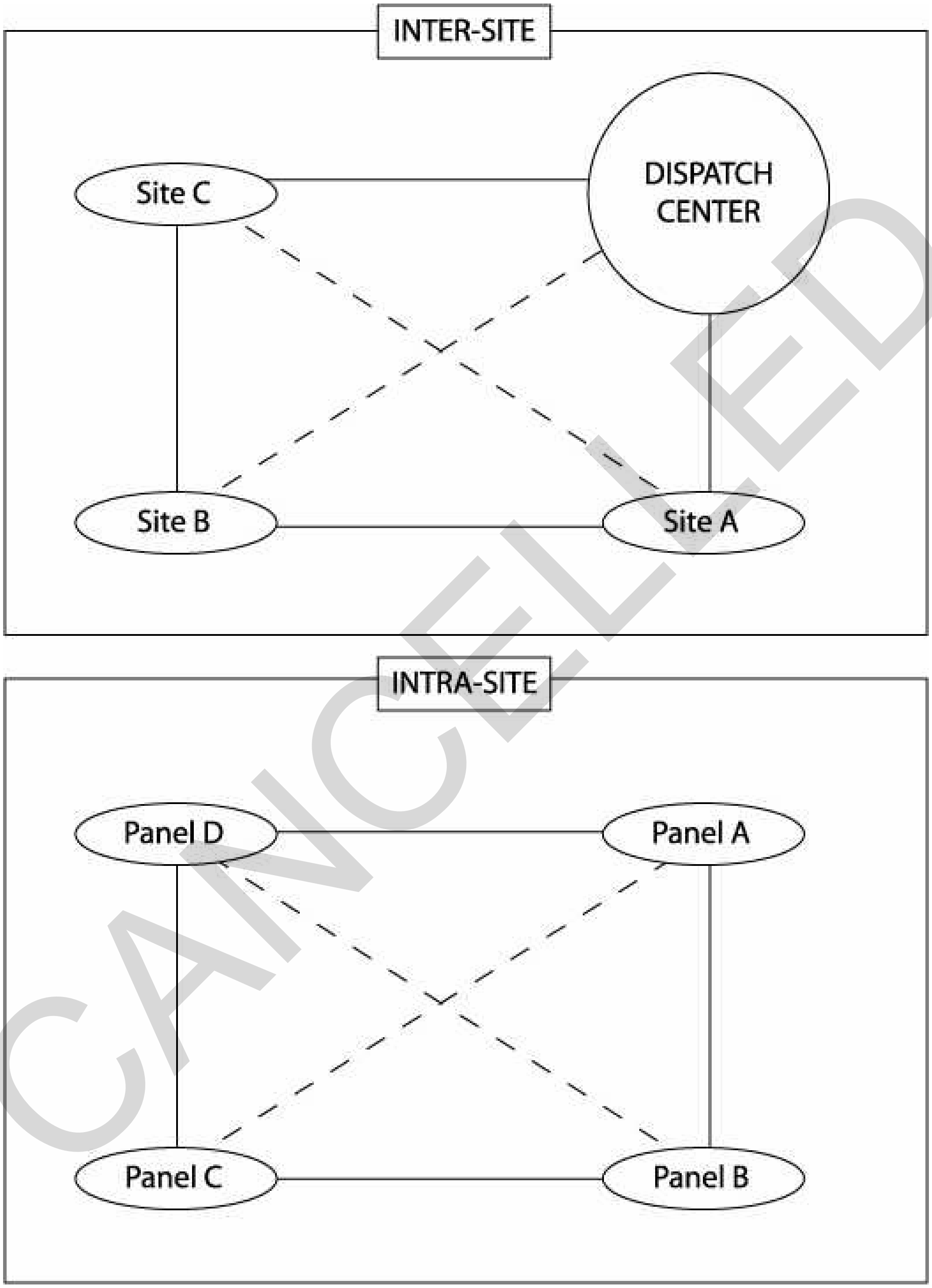


**Figure 6-3. Fully-Meshed Topographies**



## 6-5 COMMUNICATION REDUNDANCY

6-5.1 Typically the only communication redundancy made is between subsystem field panels and the system head-end. Redundancy between field panels and devices is cost prohibitive. A common method of achieving communication redundancy is achieved by running primary as well as backup RS-485 lines. If this is done, it is best to use different raceway routing schemes.

6-5.2 New product developments and improved design configurations increasingly harden communication system redundancy. This concept is currently more applicable to DTM IT (servers and telecommunication links) systems as opposed to vendor-specific ESS subsystems, such as ACS, CCTV, and IDS. Redundant communication paths are established such that if a component or link goes down, communication is maintained through an alternate communication path. While some people refer to these designs as “self-healing”, the term is really a misnomer because the failed component is still a failed component. Alternate communication paths are employed until the fault can be corrected.

## 6-6 TRANSMISSION MODES/PROTOCOLS

6-6.1 Several modes and protocols exist for electronic security data transmission. These include serial communication (RS-485, RS-232), network communication using Ethernet or TCP/IP protocol, dial-up modem, T-1 line, and wireless.

## 6-7 TRANSMISSION MEDIA

6-7.1 **Hardwired**. Hardwired refers to using dedicated proprietary (DoD-owned) conductors to transmit data/video between DTM nodes**.** Dedicated conductors can be copper or fiber-optic.

6-7.1.1 **Copper Conductors**. Generally, copper conductors can be run to 750 feet using standard RG-59/U connectors. Use of RJ-11/U conductors can extend that distance to 1,500 feet. RJ-6 should be used for longer distances. (A robust design makes use of RG-6/U, 100% double-shielded cable for outdoor applications.) These distances are general guidelines. Changes in technology permit longer distances using repeaters. Disadvantages of copper conductors include susceptibility to electromagnetic interference, radio-frequency interference and damage from lightning strikes.

6-7.1.2 **Fiber Optic**. Fiber optic allows transmission over longer distances by using light, which does not have the higher resistance loss over distance of copper conductors. Furthermore, fiber optic is not affected by electromagnetic interference or lightning. The incremental cost of installing a higher quality fiber-optic line is not significantly more for a 100 Base T line than a 10 Base T line. When in doubt, the designer should err on the side of the higher quality line. Fiber optic cable comes in two varieties, single-mode and multi-mode.

6-7.1.2.1 **Single-Mode.** Light travels through the inner core of the fiber only. Single-mode allows long distance information transfer up to 100 miles. Single-mode requires use of laser transmitter source that adds to the cost. Refer to Figure 6-4.

6-7.1.2.2 **Multi-Mode.** In multi-mode configuration, light travels through the inner and outer core paths. Multi-mode is recommended for most applications less than three to four miles. Refer to Figure 6-5.

**Figure 6-4. Single-Mode Fiber Optic**

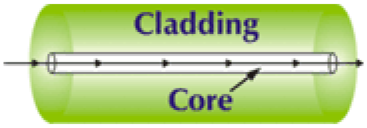
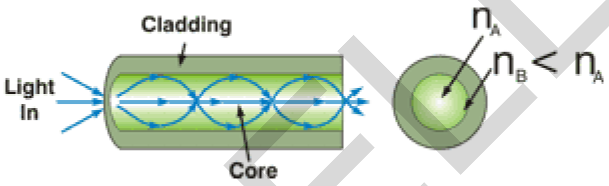


**Figure 6-5. Multi-Mode Fiber Optic**



6-7.2 **Direct Subscriber Lines (T-1 Lines).** Direct subscriber lines, also called T-1 lines, are commonly used in data transmission media systems for connecting remote sites. T-1/DS1 lines are permanent point-to-point links through public networks. The bandwidth capacity of a T-1 line is 1.544 Mbps. The cost of the leased line is dependent on distance and existing capacity or infrastructure. T-1 lines are uniquely assigned to a customer, such that only the DoD information would be transmitted over the assigned conductors (typically fiber optic).

6-7.3 **Wireless.** For security reasons, only use wireless if other media cannot be used. Wireless broadband networks make use of radio frequency transmission between towers. Wireless systems have high data transmission rates and do not require installation of cable, nor rely on existing copper infrastructure. Wireless communications are affected by line-of-sight topography and extreme weather conditions (such as rain, snow, or fog). Security can be achieved by vendor encryption and decryption at each node. The design and cost estimate must consider equipment and software for equipment and software for authentication servers and encryption systems. Some radio modem units can provide data transmission rates of several megabits per second - at ranges up to ten or more miles between modems. One disadvantage of wireless systems is the systems are susceptible to jamming.

6-7.3.1 **Frequency Allocation**. Frequency allocation or radio frequency spectrum planning is a critical issue and in some areas of the world a show-stopper. Because a frequency is allocated on a near-by base does not mean it will be authorized for the facility in question. Frequency allocation is a long lead-time item. Employment of radio frequency transmitting equipment outside of the continental United States usually requires approval by the Host nation. While there are some “worldwide license free” frequencies, host nation approval can be slow and or difficult with nuances of licensed and unlicensed equipment. Long lead times may be required for equipment that met Host nation requirements or alternative solutions to radio frequency emitting devices may have to be considered. Approval of radio frequency emitters should be an early project design consideration.

6-7.4 **Free-Space Optics (FSO).** FSO, also called free-space photonics (FSPO), refers to the transmission of modulated visible or infrared (IR) beams through the atmosphere to obtain broadband communications. Most frequently, laser beams are used. FSO operates similar to fiber optic transmission, except that information is transmitted through space rather than a fiber optic. FSO systems can function over distances of several kilometers, but does require a clear line-of-sight unless mirrors are used to reflect the light energy. FSO systems offer advantages of reduced construction cost in that fiber optic lines do not have to be installed, but there are limitations. Rain, dust, snow, fog, or smog can block the transmission path and shutdown the network.

## 6-8 TECHNOLOGY COMPARISION

6-8.1 Table 6-2 provides a comparison matrix of different DTM technologies for ESS.

6-8.2 **Explanation of Table 6-2.** Dedicated conductors are high-lighted for on-base applications and T-1 lines are highlighted for interbase applications as a general guide. Whichever method is used, initial calculations have to be made on the information transfer (bandwidth) requirements.

## 6-9 ENCRYPTION

6-9.1 Encryption of ESS DTM is an evolving area with new standards under development. Some general guidance follows.

6-9.1.1 ACS: A new emerging NFPA guide suggests that ACS inter-building information be encrypted.

6-9.1.2 CCTV MPEG and IEEE have encryption guidelines for video transmission. IEEE 802 is in draft version at this time. Federal Information Practices Standard 140 is an additional reference.

Refer to Chapter 9 for additional information on tamper protection and encryption requirements.

### Table 6-2. DTM Technologies for ESS

| | Hardwired | Leased T-1 Lines | Wireless | Free Space Optics |
|---|---|---|---|---|
| **Suitability On Base** | Recommended application. | Does not make sense when base level information infrastructure can be used. | Generally requires line of sight. | May make sense, can be used when there is line of sight. |
| **Suitability Inter Base** | Rarely achievable, because of property line boundaries. | Recommended application. Can cross property lines. | A workable application | May make sense. |
| **Initial Cost** | Dependent on distance. Principle cost is per linear foot of trenching/ conductors. | Low, which is good. Must provide interface to site's demarcation point for supplier. | Construction costs of towers and tie-ins has to be computed. | Reduced initial cost because conductors are not used. Need transmit/receive equipment. |
| **Recurring Cost** | Low, which is good. Minimal maintenance cost of installed conductors. | One T-1 line at 1.544 Mbps can be estimated at $500/month. Obtain vendor quote. | Relatively low, which is good if DoD-owned. Otherwise obtain vendor quote. | Low if DoD equipment. Leased equipment requires vendor quote. |
| **Considerations** | Best technology. Not affected by line of sight. | As good as "hardwired." Not affected by line of sight. | Generally requires line-of-sight. Approved frequencies must be used. | Requires line of sight or mirrors. |
| **Security** | Very good, especially if totally contained on DoD property. | Second or third best choice. Usually dedicated conductors are used from one provider. | Not recommended by CIA studies, but may make sense on DoD property if there is little chance of interception. | Signals can be blocked. Hard to transmit forged signals. |
| **Weather Effects** | Not affected. Best technology from weather consideration. | Not affected. As good as "hardwired." | Not as bad as free space optics, but can be affected by heavy rain and snow. | Rain, dust, snow, fog, or smog can block transmission, shutdown network. |

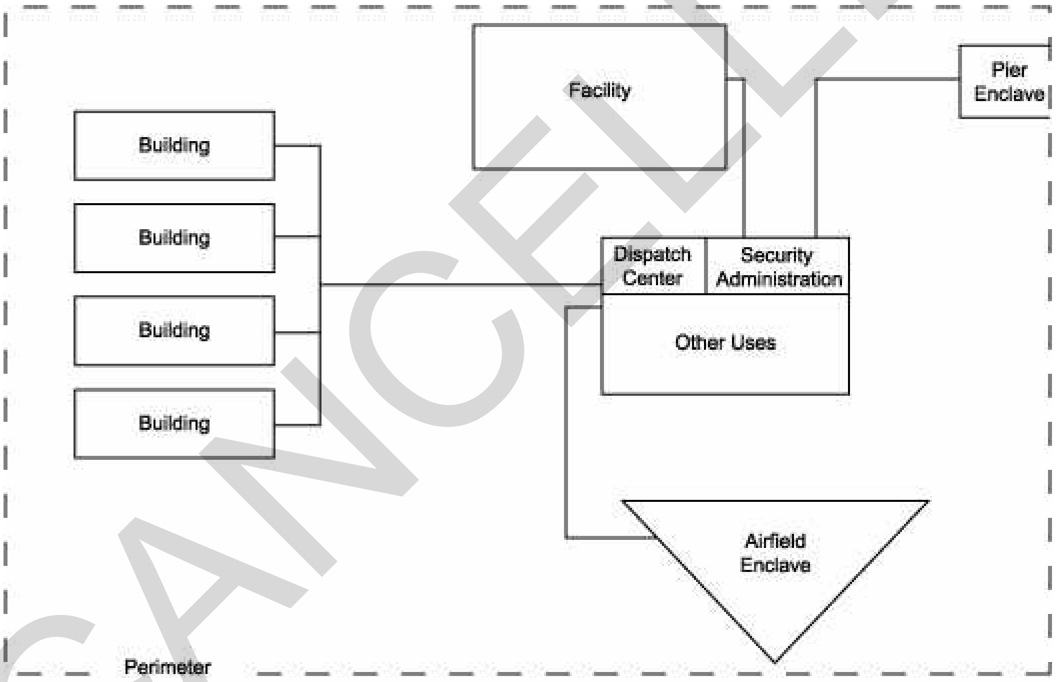
# CHAPTER 7

# DISPATCH CENTER

## 7-1 INTRODUCTION

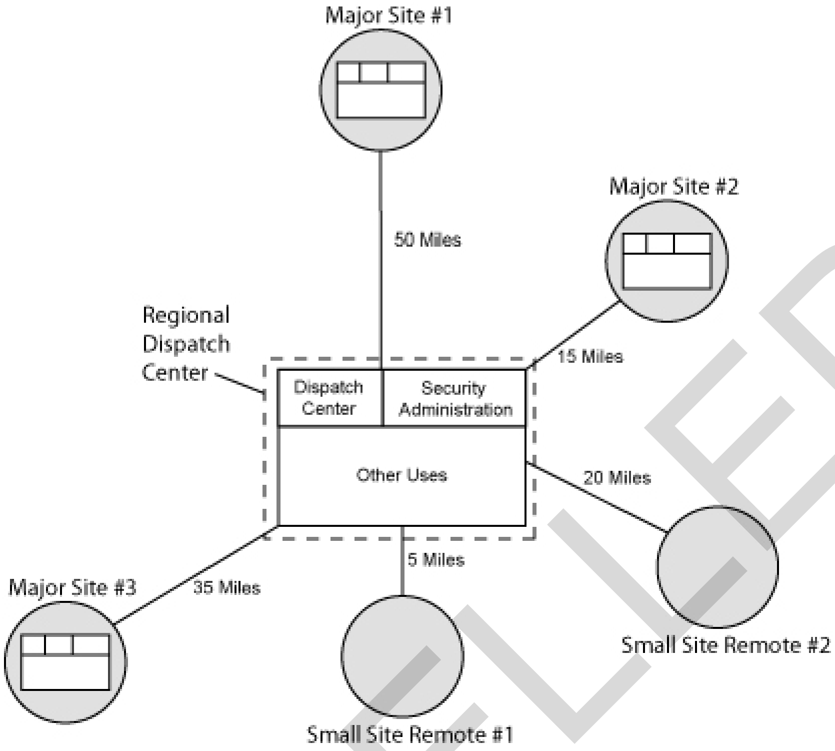
7-1.1 The Dispatch Center, also known as the Security Operations Center (SOC), Security Control Center (SCC), or Central Monitoring Station is an area that serves as a central monitoring and assessment space for the ACS, CCTV, and IDS systems. In this space, operators assess alarm conditions and determine the appropriate response, which may entail dispatching of security forces. Normally, the Dispatch Center is staffed by trained personnel 24 hours a day, seven days a week. The Dispatch Center may be co-located with other installation functions. Refer to Figure 7-1.

**Figure 7-1. Dispatch Center Centrally Located**



7-1.2 When several regional installations or sites interface and report to a centralized dispatch center, that space or building may be known as a Regional Dispatch Center (RDC). Refer to Figure 7-2.

**Figure 7-2. Example RDC**



7-1.3 Small facilities not located on a DoD installation such as Reserve Centers, medical clinics, or pharmacies may be connected to a Central Station or Police Station.

## 7-2 SPACE

7-2.1 Space programming for a Dispatch Center should consider the following:

7-2.1.1 Equipment wall space

7-2.1.2 A minimum of three-foot clearance in front ( and rear if used for service) of all electrical cabinets and enclosures (NFPA 70 requirement).

7-2.1.3 Counter space for consoles

7-2.1.4 Personnel space for each operator

7-2.1.5 Space for UPS equipment

7-2.1.6 Access requirements for maintenance or repair.

7-2.1.7 Conduit space requirements for future system wiring or enhancements.

7-2.1.8 Future growth or expansion space

## 7-3 LIGHTING

7-3.1 The Dispatch Center space should be designed for normal interior lighting levels according to the classification of the space: equipment room or Dispatch Center. Consideration should be given to selectable lighting or dimmers that allow reducing the lighting behind or near system displays. Use of dimmers or task lighting should be considered at operator's areas. Indirect lighting should also be a consideration. The design should strive for no glare of monitor screens.

## 7-4 CONSOLES

7-4.1 A determination should be made early as to how many stations are required. The layout for a simple Dispatch Center console is displayed in Figure 7-3. Although security system monitors may be co-located with other functions such as a 911 call center and fire alarm monitoring personnel, most commands find a separate administrative personal computer and printer is required in the Dispatch Center. A conceptual layout for a small to medium sized Dispatch Center is displayed in Figure 7-4.

**Figure 7-3. Sample Simple Dispatch Center Console Layout**

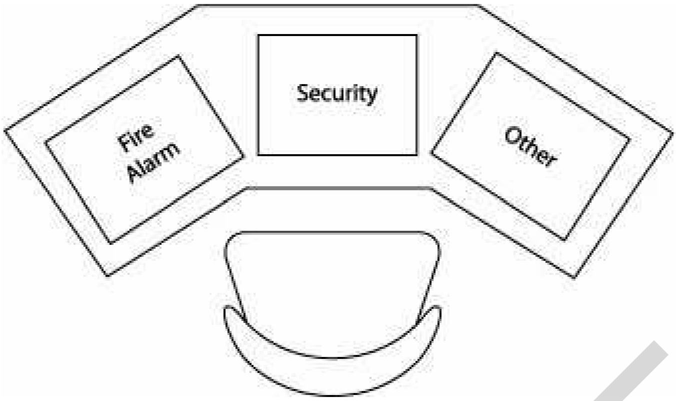
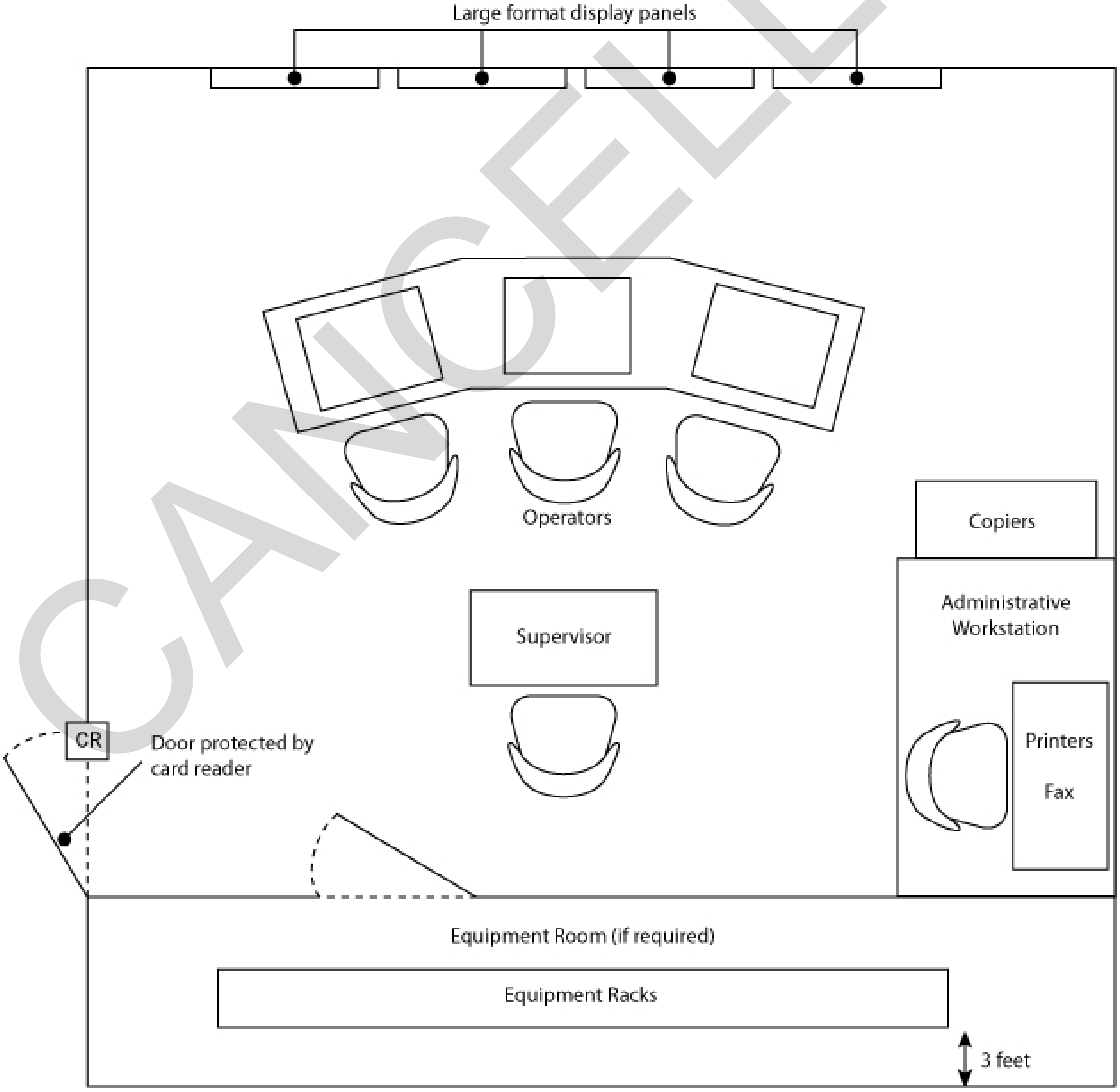


**Figure 7-4. Sample Small-Medium Dispatch Center Space Layout**


Large format display panels
Operators
Copiers
Administrative Workstation
Supervisor
CR
Door protected by card reader
Printers
Fax
Equipment Room (if required)
Equipment Racks
3 feet

## 7-5 MONITORS

7-5.1 Monitors should be ergonomically mounted. New products allow wall-mounted flat-screen plasma displays and smaller, hinged, flat monitors that can be swiveled out and adjusted for individual operators.

7-5.2 Monitors should meet the following minimum specifications:

7-5.3 **Horizontal resolution**: 450 lines of horizontal resolution at center; 700-800 TV lines offer super-high resolution.

7-5.4 **Brightness**: More than 250 lux in 100% white signal at center.

7-5.5 **Total geometric distortion**: less than 3%.

## 7-6 GROUNDING/POWER CONDITIONING

7-6.1 It is a good practice to provide a dedicated ground bus bar in the Dispatch Center for grounding the ESS panels. Refer to NFPA 70 and TIA-J-STD-607 for additional guidance on grounding and power conditioning.

## 7-7 HVAC

7-7.1 Typical environmental conditions for a Dispatch Center are as follows:

7-7.2 72 degrees Fahrenheit plus/minus five degrees.

7-7.3 50% Relative Humidity (RH) plus/minus 10%**.** If the relative humidity drops below 30%, there can be equipment problems due to abnormally high level of static electricity. Conversely, too high a humidity can result in condensation, which may cause electrical shorting or corrosion problems.

7-7.4 HVAC heat/cooling loads can be calculated by considering these heat loads:

7-7.5 **Personnel and equipment**. The average staffing count of personnel in conjunction with the kilowatt (kw) load of associated electrical equipment such as DVRs and ESS servers as well as internal lighting loads**.** For personnel, ASHRAE 62 recommends 20 cfm flowrate per occupant. Refer to NMCI UFC 3-500-10N and utilize equipment loads based on the room configuration.

7-7.6 **Shell load**. Shell load considers the perimeter walls, ceilings, windows, and associated solar gains of the external surfaces.

7-7.7 **Outside air**. Heating or cooling as required for the climatic conditions of the Dispatch Center location.

7-7.8 Components to consider are air handlers, ductwork, inlets and outlets (diffusers and grills), as well as heating and cooling sources.

7-7.9 Dispatch Centers lend themselves to “packaged HVAC equipment systems” because of the relatively low heat load, as opposed to centralized systems for bigger, more complex building types**.**

## 7-8 SUPPORT ROOMS

7-8.1 A good practice is to plan for nearby support equipment room space to the Dispatch Center. This room can be used to house local ESS equipment such as digital recording equipment (DVRs), local security panels, and termination cabinets. Additional HVAC capability may be required in dedicated equipment spaces due to the heat generated by equipment.

# CHAPTER 8

# ESS SUBSYSTEM INTEGRATION

## 8-1 OVERVIEW

8-1.1 Since the different subsystems of a facility's total ESS are drawn on a number of different technologies (i.e. camera technology, biometric technology, microwave intrusion technology, and information transfer technology), the manufacturers of subsystems tend to be uniquely different**.** As a result, system integration or making the subsystems and components "talk to each other" reliably and consistently is a major portion of an ESS design**.** The purpose of this chapter is to briefly consider some of the system integration issues associated with an ESS.

## 8-2 COMMUNICATION FROM THE IDS TO THE ACS

8-2.1 As covered in Chapter Two, "Electronic Security System (ESS) Overview," for a simple system, the IDS may already be an integral part of the ACS**.** In these intermediate systems (depicted in Figure 2-7), basic intrusion detection devices are brought into a combined ACS/IDS system as digital inputs on local security panels. All that is required is to allocate digital input points in the closest security panels and program the ACS to provide an alarm on event.

## 8-3 COMMUNICATION FROM THE IDS[1] TO THE CCTV SYSTEM

8-3.1 Once an intrusion is detected (i.e. door forced open or perimeter fence or microwave intercept), it is generally the practice to make sure the event is being viewed and recorded. Interface of the IDS to the CCTV system can occur through several different means: hardwired conductors, serial communications, and networked connections as discussed below. Activation of an intrusion detection alarm results in an audible alarm that gets the operators attention.

8-3.2 **Hardwired Conductors**. Older technology; still effective for simple installations. In this case, copper conductor wiring is taken as digital outputs from the IDS or combined ACS/IDS and connected as inputs to the CCTV system to initiate camera recording and if required – panning to a pre-set location. In the most basic approach, this design requires a pair of wires for each alarm notification output signal.

8-3.3 **Serial Communications**. RS232 (a two-wire shielded 16 AWG conductor.) In theory, this is the same principle of operation as the hardwired method with an improvement in that a single RS232 conductor pair can handle several camera signals. It is most easily done when the CCTV and IDS (or combined ACS/IDS) are made by the same vendor, but can be done with different vendors, but requires writing or availability

[1] or combined ACS/IDS

of software drivers. While slightly more complicated than the hardwired approach, this method has the advantage of reduced wiring costs.

8-3.4 **Networked Connections**. Current COTS security systems are moving in the direction of networked inter-system design. If this method is selected, a separate security network should be installed. In this approach, Ethernet cable is routed to the headend equipment and a static internet protocol (IP) address for the CCTV and IDS or combined IDS/ACS subsystems. The network connection allows communication between the remote equipment and a server or desktop personal computer (PC), usually located in the Dispatch Center. The desktop PC will have a security program that accesses remote equipment through IP addresses provided during setup. The security program allows the user to access CCTV and IDS/ACS information. When using this approach, having adequate bandwidth is important due to the large amount required for video information. As mentioned, network security is also of paramount importance and for DoD projects a dedicated security network is recommended. Cost savings of reduced point-to-point wiring have to be compared to possible new costs of installing a dedicated network. A drawback to this approach is that typically the manufacturer of both the CCTV and IDS/ACS have to be the same vendor unless compatible software drivers for allowing both systems to talk to each other are available or created.

8-3.4.1 Networked security systems are typically a Proprietary Security Network. A Proprietary Security network is a completely self contained dedicated local area network (LAN) with security system software installed and run on a host server (computer). Proprietary Security Networks are dedicated to the ESS with no outside (Internet, LAN, or WAN) connections. All networks must meet the applicable DoD and service component certification policies and procedures. A unique user ID and password is required for each individual granted access to the IDS host computer. Public Key Infrastructure (PKI) certificates may be used in lieu of User ID and password for positive authentication. Positive authentication methods must be in accordance with published DoD policy and procedures. System must monitor and log all network and ESS component access attempts and all changes to ESS application using auditing and network intrusion detection software or similar enhancements. If connection to an outside LAN/WAN is a system requirement, the system would not be considered a Proprietary Security Network and the following additional requirements would apply:

- Encrypt all host server communications to the LAN/WAN using a NIST-approved algorithm with a minimum of 128-bit encryption.
- Protect the system from compromise with firewalls, or similar enhancements that are configured to only allow data transfers between ESS components and authorized monitoring components.

## 8-4 COMMUNICATION FROM THE CCTV SYSTEM TO THE ACS

8-4.1 For those limited applications where the CCTV system is being used as an intrusion detection methodology (primarily interior camera locations), the CCTV system can be configured to provide an alarm input to the ACS system.

## 8-5 COMMUNICATION FROM THE ACS TO THE DISPATCH CENTER

8-5.1 Most alarm signals are usually transmitted from the ACS to the Dispatch Center.

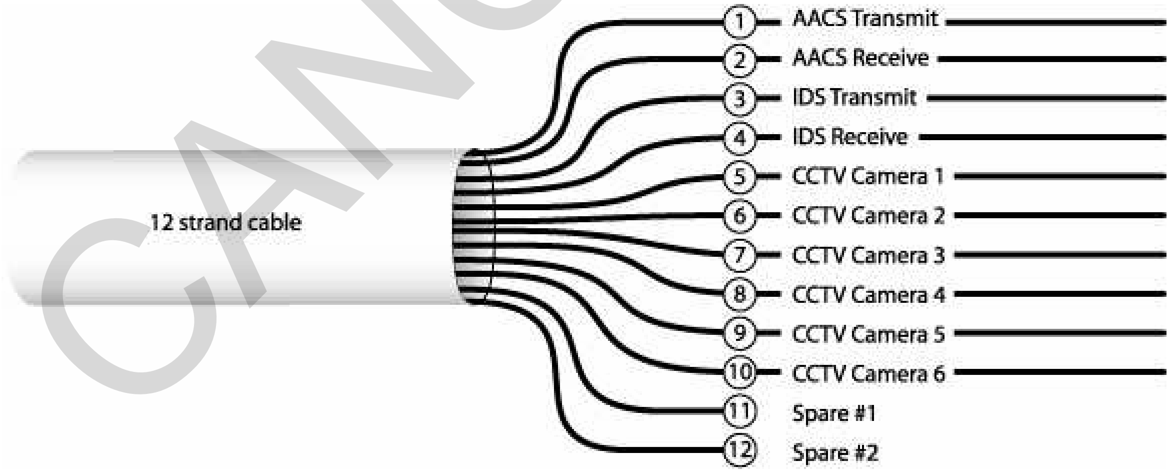
## 8-6 COMMUNICATION FROM THE DISPATCH CENTER TO THE ACS

8-6.1 Some projects require or are designed such that door unlock signals can be manually generated from the Dispatch Center. In those cases a door open signal is an output from a device in the Dispatch Center to the ACS.

## 8-7 BANDWIDTH ANALYSIS

8-7.1 A study should be made of the bandwidth communication requirements for each subsystem through the DTM to the Dispatch Center. Typically, the CCTV system will have the highest requirement, but there will be data communications – normally in the range of kilo-bytes-per-second (kbps) – for the ACS system and IDS systems. The DTM may make use of the base Information Technology systems. If base fiber optic is used, a good design detail is a fiber schedule showing which fibers on which cables are dedicated to the DTM or other systems. Plan on one fiber pair for ACS communication – one fiber transmit and one receive. Similarly, plan on one fiber pair for required IDS communications. CCTV typically only requires one fiber per camera. For PTZ cameras, one wavelength on the fiber can be used for the video signal and another wavelength on the same fiber can be used for the PTZ control signals. Refer to Figure 8-1 for a sample illustration.

**Figure 8-1. Sample DTM System Detail**



8-7.2 Coordinate with the base communications officer (information technology) or for Base Level Information Infrastructure and Defense Information Infrastructure.

8-7.3 Design Guidance on IT System Coordination. Fiber optic cables typically come in multiples of twelve strands, with 12-strand and 24-strand fiber optic cable being very common. While there are no technical limitations on combining ESS with other base systems, such as IT or Instrumentation and Control, it is preferable to keep ESS fibers dedicated for security purposes only from a security standpoint. If other unrelated systems are on a common fiber, other vendors or organizations will have closer access to the security communications.  Plan for future expansion (provide a minimum of 20%) spare capacity (fibers).

# CHAPTER 9

# GENERAL REQUIREMENTS AND CROSS-DISCIPLINE COORDINATION

## 9-1 GENERAL REQUIREMENTS

9-1.1 **General.** The highest security should be applied close to the critical asset. Avoid burdening the entire general population with the highest level of security. Other considerations include:

9-1.1.1 All PCUs should be located within the secure area.

9-1.1.2 Enunciators, controls and displays subsystems should be located in restricted areas and closed off from public view.

9-1.2 **Certifications and Listings.** Equipment and systems should be proven with a demonstrated history of reliability. One mean of achieving this criteria is to specify listed or certified products/systems such as:

9-1.2.1 United States: Underwriter's Laboratory (UL)or similar nationally recognized testing and listing agency. Refer to UL 294 for a standard on ACS.

9-1.2.2 European Union CE listing. CE certifications, referred to as "CE Marking" may be required by the Host Nation for systems provided in Europe. The letters "CE" are an abbreviation of a French phrase "Conformite Europeene". The marking indicates that the manufacturer has conformed with all the obligations required by the European Union (EU) marketplace.

9-1.3 **System Acceptance Testing.** This section discusses system testing and ownership acceptance procedures and provides sample system commissioning documents.

9-1.3.1 **Labeling.** Major equipment should have labels to identify the system and device. Cables should be labeled at origination, termination, and within enclosures using permanent labels.

9-1.3.2 **Test Documentation and Acceptance Forms.** Normally the ESS designer's technical specifications or Scope-of-Work will include requirements for test documentation as prescribed by other DoD mandates. Currently a UFC on testing procedures is under development.

9-1.3.3 **Pre-Test walkthrough.** A pre-test walkthrough should be performed by the contractor before the final acceptance testing. This allows the final acceptance test to go smoothly and prevents mishaps and additional testing.

9-1.3.4 **Training.** Consideration should be given to administrator and operator training. The ESS designer should consider adding the number of hours required to the appropriate portion of system specifications. Typically, several training sessions with a minimum of one per work shift should be considered. It is a good practice to define some performance criteria such as “upon training completion, the tenant command should be able to unilaterally make additions or deletions to the ACS database.”

### 9-1.4 Operation and Maintenance

9-1.4.1 **Overview**. In specifying ESS, the designer needs to consider maintenance, service, repair, and sustainability of systems and the associated components. Systems with arduous requirements should be reconsidered.

9-1.4.2 **Spare Capacity.** An ESS should have the capability to be easily expanded or modified for simple changes, such as adding a card reader or camera, over the near-term life of the system. Accordingly, the ESS designer should plan for a nominal 20% expansion capacity when designing a new system.

## 9-2 GENERAL COORDINATION

9-2.1 Throughout the planning and design process the designer should coordinate closely with security (Physical Security Officer) and anti-terrorism personnel (Antiterrorism Officer), end-users, base communications officer (information technology), and fire and safety personnel.

## 9-3 CIVIL COORDINATION

9-3.1 **Gate Control (Vehicle Gates and Sally Ports).** A sally port is a holding port where vehicles are located. Sally ports may require control hardware for interlocking gates. Refer to UFC 4-012.1 (Security Engineering: Entry Control Facilities/Access Control Points) for more information on sally ports and entry control points.

9-3.2 **Underground Site Work.** Inter-building DTM communications are often made by buried direct conductors. Underground site work needs to coordinated with existing civil drawings and buried utilities.

## 9-4 ARCHITECTURAL COORDINATION

9-4.1 **Importance of Coordination**. Past experience shows that the biggest disconnect in project design and construction costs is due to lack of coordination between commands, security, engineers, and ESS installation personnel. It is imperative that planned ESS component locations be identified early in initial design and planning stages in order to coordinate conduit installation and electronic module interface requirements for security locks and equipment. Additionally, coordination in the project programming stage will give persons responsible for collateral equipment the time necessary to plan for the facility’s necessary equipment.

Detailed door-by-door coordination reviews should be conducted during design development and creation of construction documents.

9-4.2 Other architectural issues that need to be considered include balancing security with convenience, entries and exits, life safety code considerations, space planning, doors, and door locks. These are discussed in the following sections.

9-4.3 **Balance of Security With Convenience**. There is a natural conflict between making a facility as convenient as possible for operation and maintaining a secure facility. Convenience should be considered during the different phases of the design review; however, the requirement for security should never be sacrificed for convenience. Proper security controls will reduce the flow rate and ease of ingress and egress in and out of a facility. These issues must be addressed in initial planning to facilitate additional entry points or administrative requirements.

9-4.4 **Entries and Exits**. In general, provide separate entries and exits. Establish the number of entry/exit points consistent with security and safety guidelines. For an SCIF only one entrance is allowed unless approved by the Cognizant Security Authority.

9-4.4.1 Use of external door hardware is prohibited on SCIFs (with the exception of the SCIF entrance).

9-4.4.2 Obtain a copy of the facility’s code diagram and access control and develop an emergency action plan for coordination of security at door openings.

9-4.5 **Space Planning**. Early in the project, architectural issues for Dispatch Center space, wall space for security panels and floor space for ESS equipment racks needs to be discussed. Normally, security panels will go in telecommunication rooms. The ESS designer should coordinate with the telecommunications system designer for space requirements in the telecommunications room.

9-4.5.1 DoD criteria requires that telecommunication rooms are separate from electrical equipment rooms. These spaces will be climate controlled separately from adjacent spaces.

9-4.6 **Doors**. Entry control is achieved through locking an opening such as a door or gate**.** Using the example of card reader controlled doors, the door is controlled through a door locking mechanism**.** When deciding which locking mechanism to use a decision must be made as to whether the door is “fail-safe” or “fail-secure.” While most facilities will make all egress doors able to be opened from the “secure-side” in the egress path during a fire emergency, there are options as to whether the controlled door is able to be open from the “public-side.”

9-4.6.1 **Fail-Safe.** Fail-safe doors fail open on loss of electrical power. This means that if power is lost the door hardware is configured such that the door can be opened by anyone from the “public-side.” While affording great convenience, this configuration is vulnerable to intrusion during a power-loss event.

9-4.6.2 **Fail-Secure.** Fail-secure refers to entry from the public-side. Fail-secure doors fail shut on loss of electrical power. This means that if power is lost the door hardware is configured such that the door cannot be opened from the public-side.

These doors need to be keyed such that they can be manually unlocked by appropriate response personnel until the security alarm panel and electrical power can be reset. Emergency doors are required to be able to be opened for exiting during a fire-emergency except for certain restricted institutional facilities (prisons and high-security hospitals).

9-4.6.3 **Door Coordination.** Door control impacts (door hardware needs or changes) are sometimes overlooked in project construction cost estimates. Inventory of doors and assessment of door and hardware suitability should be an early design issue for assessing project door interface requirements. Door coordination is one of the most frequent (and costly) problem areas on security projects. It is important that the ESS designer coordinate with the project architect to ensure that the proper door hardware is specified and installed.

9-4.6.4 **Life Safety Codes.** Great care should be taken in designing access control for doors. Refer to the Life Safety Code and Means for Egress for Buildings and Structures for code guidance on egress and ingress doors.

9-4.6.5 **Recommendation**. Unless there is a compelling convenience reason for making a door fail-safe, most ESS projects are designed such that the door hardware is Fail-Secure.

### 9-4.7 **Door Locks**

9-4.7.1 **Electric locks**. The electric lock is a very secure method to control a door. An electric lock actuates the door bolt. For very secure applications dual locks can be used (for example, a retractable bolt on and at the top of the door frame and an additional retractable bolt on the side of the door). In some cases, power is applied to engage the handle, so the user can retract the bolt vice the electric operator actually retracting the bolt. Most electric locks can have built-in position switches and request-to-exit hardware. While offering a high security level, electric locks carry a cost premium. A special door hinge, that can accommodate a wiring harness and internal hardware to the door, is required. For retrofit applications, electric locks usually require purchase of a new door.

9-4.7.2 **Electric strikes**. The difference between an electric strike and an electric lock is the mechanism that is activated at the door. In an electric-lock door the bolt is moved. In an electric-strike door the bolt remains stationary and the strike (or cover latch) is retracted. As in electric locks, electric strikes can be configured for fail-safe or fail-secure operation. The logic is the same. In fail-safe configuration the strike retracts when de-energized on loss of power. This allows the door to be opened from the public side. In fail-secure configuration the strike remains in place causing the door to be locked from the public side and requires manual key entry to unlock the door from the public side. Again, as with electric locks, unimpeded access is allowed for in the direction of egress by manual activation of the door handle/lever when exiting from the secure side. For retrofit situations electric strikes rarely require door replacement and can often be done without replacing the doorframe.

9-4.7.2.1 Electric strikes should be protected with a cover guard. Exposed electric strikes can be over-ridden (pried open) by an intruder with a pocket knife screwdriver.

9-4.7.3 **Magnetic locks**. The magnetic lock is popular because it can be easily retrofitted to existing doors**.** The magnetic lock is surface-mounted to the door and doorframe**.** Power is applied to magnets continuously to hold the door closed**.** Magnetic locks are normally fail-safe (they can be fail-secure through the use of a solenoid)**.** This may be a problem for unstaffed facilities in the event of a power disruption that will leave the site unsecured until security personnel arrive or power is restored.

9-4.7.3.1 Magnetic locks do have a security disadvantage**.** In the United States, continuous locking of exit doors is not permitted**.** (For more information refer to NPFA 101, Life Safety Code.) Doors equipped with magnetic locks are required to have one manual device (such as a Request-to-Exit, or REX button) and an automatic sensor (typically a passive infrared sensor, PIR) to override the door lock signal when someone approaches the door in the exit direction. While enhancing overall building safety, the addition of these extra devices allows possible compromise of the door lock in the following scenario:

1. Person A in on the secure side of the door and walks into the field-of-view

2. The door lock signal is shunted by the activated automatic sensor.

3. Person B (located on the public side of the door) can open the door and breach the security of the locked opening.

Magnetic locks should be the designer’s last choice for door locking mechanisms and should probably only be used on a retrofit project.

## 9-5 LIFE SAFETY CODE CONSIDERATIONS

9-5.1 Applicable life safety and existing codes/standards must be met. In the event of an emergency, building occupants must be able to follow emergency procedures quickly and safely. The ESS designer must coordinate with the building architect (for items such as exit plan considerations) and the building fire protection engineer (for fire alarm system integration) to implement security without comprising life safety code standards. This requires close coordination and at times creative architectural and security design solutions to implement the requirements of both safety and security. Physical security system designs need to be coordinated with and comply with NFPA 101 and the Americans with Disabilities Act (ADA).

## 9-6 ELECTRICAL COORDINATION

9-6.1 Electrical issues that need to be considered include power, backup power, grounding, bonding, lightning protection, cable type, electromagnetic interference, tamper protection, voltage drop considerations, power reliability, harmonics, raceway, labeling, shielding, fire alarm system interface, and lighting. These are discussed in the following sections.

9-6.2 **Power**. ESS loads should be fed from distribution panels within the protected area. A good practice is to use distribution panels with dedicated security system breakers that can be locked. No other load should be fed from breakers feeding ESS loads. In addition to the panel nameplate, provide a label with the following inscription: "Security System Breaker Within." Label shall be constructed and fastened identical to the panel nameplate, except the label shall be red laminated plastic with white-center core.

9-6.3 **Backup Power**

9-6.3.1 **Battery Backup**. The minimum requirement for battery backup for an IDS and its monitoring station is eight hours. If primary power is subject to being out for longer periods, increase backup capacity accordingly. The requirement for battery backup for a SCIF and its monitoring station is 24 hours. The battery backup requirement for a SCIF can be reduced if the system is on a generator. Monitoring stations must have visible and audible indicators to inform system operators of failure of a power source, a change in power source, and the location of the failure or change.

9-6.3.2 **Generator and Uninterruptible Power Supply.** ESS components are primarily low voltage equipment devices and are easily supplied by battery backup. This UFC is not intended to require a central UPS or generator to back up an ESS. When an emergency power generator exists or is planned for other requirements, batteries may serve as the backup power means during the diesel generator startup time period.

9-6.3.3 **Backup Power for CCTV**. Depending on criticality of an asset and the availability of security forces to assess alarms, consideration should be given for providing backup power for CCTV systems used for assessing alarm conditions.

9-6.3.3.1 Provide battery backup for CCTV system platforms that are used as an IDS sensor.

9-6.3.4 Battery calculations should be required to verify the system's backup batteries have the proper capacity.

9-6.4 **Grounding, Bonding, and Lightning Protection**. Refer to UFC 3-520-01, TIA J-STD-607, NFPA 70,and NFPA 780 as applicable.

9-6.5 **Cable Type**. In general, data signals should be provided in shielded cable. Data communication signals are sensitive to changes in capacitance and resistance associated with different cable types**.** Digital "1s" and "0s" trigger on sharp LRC (inductance, resistance, capacitance) time constants**.** The ESS designer should specify low capacitance cable and sufficient twists per foot that meet manufacturers' specifications. Dry contact signals can be provided in unshielded cable to lower the cost of installation.

9-6.6 **Surge Protection**. Refer to UFC 3-520-01.

9-6.7 **Electromagnetic Interference (EMI).** Interference can be introduced to unprotected communication lines that are in close proximity to electrical power wiring, radio frequency sources, large electric motors, generators, induction heaters, power transformers, welding equipment, and electronic ballasts. Protection from EMI includes avoiding the sources of the interference by physical separation or shielding wire lines by means of specialty wiring (coaxial, twisted shielded (foil) pairs, and metal sheathed cables), and metallic conduit systems.

9-6.8 **Tamper Protection**. Tamper protection for ESS can be physical protection, line supervision, encryption, and/or tamper alarming of enclosures and components. All intrusion detection, access control, assessment systems, and their associated data transmission media must be protected commensurate with the classification of the asset being protected. All intrusion detection sensors and access control readers must have tamper resistant enclosures, and integral tamper protection switches. All enclosures, cabinets, housings, and boxes, having hinged doors or removable covers that contain processors or connections must have tamper protection switches. All tamper alarm signals must be monitored continuously whether the system is in the access or secure mode of operation.

9-6.8.1 **Signal and DTM Supervision.** Line supervision is a term used to describe the various techniques that are designed to detect or inhibit manipulation of communication networks. All signal and DTM lines must incorporate some level of line supervision. Line supervision for ESS must detect and annunciate communication interruptions or compromised communications between field devices and the associated CPU (or PCU). Field device signals must be supervised by monitoring the circuit and initiate an alarm in response to opening, closing, shorting, or grounding of the signal. All DTM must be supervised by the appropriate level of encryption and must initiate an alarm upon any manipulation or disruption of the signal.

9-6.8.2 **Encryption.** Encryption is where the transmission of the signal is supervised by employing a data-encryption standard that applies a specific algorithm to alter the appearance of the data. For high security areas (Level Two and Three Restricted Areas), AA&E and controlled access areas that process Secret or above classified material, the encryption must be a 128-bit format, which complies with the National Institute for Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 140-2. Systems protecting all other assets must meet UL 1076 Class AA line security standards.

9-6.8.3 **Physical Protection of ESS Raceway and Enclosures.** Interior and exterior ESS should be physically protected as described below.

9-6.8.4 **Physical Protection of Exterior ESS.** Physically protect exterior ESS. All exterior intrusion detection sensors and access control readers must have tamper resistant enclosures and integral tamper protection switches. All enclosures, cabinets, housings, boxes, and fittings having hinged doors or removable covers that are protected by employed sensors must be locked, welded, brazed, or secured with tamper resistant security fasteners and be tamper-alarmed. Route exterior ESS sensor communication and power cables that are not directly protected by sensors by one of the following methods:

9-6.8.5 In rigid metal conduit.

9-6.8.6 In concrete encased duct.

9-6.8.7 In direct buried conduit to a minimum of twenty-four inches (0.6 meters) below finished grade.

9-6.8.8 Suspended at a minimum of 15.5 feet (4.5 meters) above the finished grade.

9-6.9 **Physical Protection of Interior ESS.** All interior intrusion detection sensors and access control readers must have integral tamper protection switches. All intrusion detection sensors, access control readers, and assessment equipment located outside controlled areas must have tamper resistant enclosures. All intrusion detection sensors and access control system cabling should be routed within the controlled area. If the cables transverse an uncontrolled area, the cables must be locked, welded, brazed, or secured with tamper resistant security fastners. Additionally, the following design criteria needs to be applied:

9-6.9.1 All ESS control and DTM associated with the protection of high security areas (Level Two and Three Restricted Areas), AA&E and controlled areas that process Secret or higher classified information, must be enclosed in rigid metal conduit.

9-6.9.2 All enclosures, cabinets, housings, boxes, and fittings having hinged doors or removable covers must be locked, welded, brazed, or secured with tamper resistant security fastners and be tamper-alarmed.

9-6.9.3 Any metallic conduit that leaves an area that processes classified information such as a SCIF must be decoupled (insert of nonmetallic conduit) when existing the area.

9-6.9.4 For areas used for handling, storing, production, renovation, and shipping of ammunition and explosives, metallic conduit must be run underground for at least fifty feet from the structure. The shielded cable or conduit must also be bonded to primary and secondary ground girdles where they cross.

9-6.10 **Radio Frequencies.** RF systems must employ some form of tamper protection such as:

9-6.10.1 The security system must use dedicated frequencies to transmit ESS alarm data.

9-6.10.2 The system must detect and report intentional and unintentional jamming attempts.

9-6.10.3 The system must transmit ESS alarms sent by non-hardware links even when they occur during “off-air” periods caused by maintenance or failure.

9-6.11 **Voltage Drop Considerations.** Standard voltage drop calculations need to be made by the designer for calculating ESS conductor size. This is especially important for CCTV cameras, which may be located some distance from interior termination cabinets and will probably be outside. The system designer should strive for a voltage drop of 10% or less. To calculate voltage drop, use this formula:

$$VD = .2 \text{ x } IL \text{ x}1.26^{(AWG-10)}$$

Where:

IL = Load Current

VD = Voltage Drop in volts per 100 foot circuit length (see Table 9-1)

AWG = American Wire Gauge

**Table 9-1. Voltage Drop**

| Guage (AWG) | .5 AMPS Load Current | 1 AMP Load Current | 2 AMPS Load Current | 4 AMPS Load Current | 10 AMPS Load Current |
|---|---|---|---|---|---|
| **10** | 0.10 | 0.20 | 0.40 | 0.80 | 2.00 |
| **11** | 0.13 | 0.25 | 0.50 | 1.00 | 2.52 |
| **12** | 0.16 | 0.32 | 0.64 | 1.27 | 3.18 |
| **13** | 0.20 | 0.40 | 0.80 | 1.40 | 4.00 |
| **14** | 0.25 | 0.50 | 1.01 | 2.00 | 5.06 |
| **15** | 0.32 | 0.64 | 1.27 | 2.54 | 6.95 |
| **16** | 0.40 | 0.80 | 1.60 | 3.20 | 8.00 |
| **17** | 0.50 | 1.00 | 2.02 | 4.04 | 10.00 |
| **18** | 0.64 | 1.27 | 2.54 | 5.06 | 12.71 |
| **19** | 0.80 | 1.60 | 3.20 | 6.40 | 16.01 |
| **20** | 1.01 | 2.02 | 4.03 | 8.07 | 20.12 |
| **21** | 1.27 | 2.54 | 5.00 | 10.17 | 25.42 |
| **22** | 1.60 | 3.20 | 6.40 | 12.01 | 32.07 |

9-6.11.1 To illustrate voltage drop calculations, consider the example of a 2 amp, 24 volt camera located 300 feet from the power supply. Figure 9-1 shows two attempts.

**Figure 9-1. Attempts 1 and 2**

**Attempt 1—Try 14 AWG Cable**. From chart, 1.01 voltage drop x 3 (for 300 feet) = 3.03 volts = 12.6% drop. *No good*.

**Attempt 2—Try 12 AWG Cable**. 0.64 voltage drop x 3 = 1.92 volts = 12.6 = 8% drop. *Good*.

9-6.11.2 For exterior cameras such as parking lot surveillance cameras, higher wire gauges may be required. In one example of a long distance run, 6 AWG was used to reach the first camera. After that distance, 12 AWG was found to be adequate to power the subsequent near-by cameras.

9-6.12 **Harmonics**. Harmonics in a power system are typically the odd multiples of 60 Hz such as 180 Hz and 300 Hz and are generated by switching power supplies such as in a computer, by adjustable frequency motor drives, by lighting ballasts, by UPS systems, by electric welders, and by other rectifier type equipment. Harmonics in a system are measured in total harmonic distortion (THD).

9-6.12.1 Harmonics in a power system can cause overheating of cables and equipment along with false operations. NFPA 70 requires designs to consider harmonics and IEEE 519 is a reference standard. When a neutral of a multiphase feed has significant harmonics, it is to be oversized. UL and the IEEE both have methods for de-rating standard transformers for harmonics.

9-6.12.2 Mitigation of harmonics involves either isolating the harmonic source from the rest of the power system or in isolating sensitive equipment from the harmonics**.** Methods of mitigation involve use of oversized/de-rated standard transformers or harmonic K-rated transformers (K4 or K13 being common), use of oversized neutrals in distribution systems (full size is adequate for feeds to individual equipment), use of input line reactors or output filters (usually on motor drives), and use of surge suppressors at panelboards, in wall receptacles, in power bars, or built into the input of ends loads, such as a security panel.

9-6.12.3 To further reduce electrical noise, a copper equipment ground sized per NFPA 70 (unless the cable is already shielded) and copper grounding electrode conductors sized per NFPA 70 should be run in raceways in addition to bonding metallic raceways and enclosures together.

9-6.13 **Raceway.** All conduit, wireway, and raceway shall meet the requirements of NFPA 70.

9-6.13.1 Conduit runs shall have a maximum of three 90-degree bends or any combination of bends not-to-exceed 270 degrees.

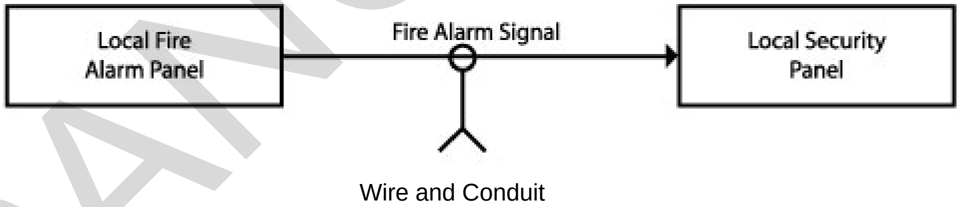
9-6.13.2 All conduit and cabling associated with the ESS should not extend beyond the perimeter of the protected area.

9-6.14 **Labeling**. Cables should be labeled at origination, termination, entry into and exit from enclosures with permanent labels.

9-6.15 **Shielding**. When required, shielded cable should only be grounded at one end – typically back at the local security panel – to prevent open loop grounds. A common question is whether or not cables in metallic conduit are required to use shielded cable**.** If there is more than one communications cable in the metallic conduit, the answer is yes – the cables should be shielded. Most manufacturers specify shielded cable such as the cable running out to card readers. The designer should follow the manufacturer's recommendations.

9-6.16 **Fire Alarm System Interface**. In the United States most egress doors are required to unlock (in the path of emergency egress) in the event of a fire emergency. (Note: certain institutional facilities are exempt from this automatic door-unlock requirement, for example, prisons or high-security hospitals.) Methods vary on how this may be accomplished. If free egress hardware is supplied (which is possible when electric locks or electric strikes are used), then that is all that is required. If magnetic locks are supplied, this life safety function has to be achieved by interfacing the ACS with the fire alarm system. Where doors are locked (electrically by magnetic locks or other devices not supplied with free exit hardware), the interface shown in Figure 9-2 should be specified in the design.

**Figure 9-2. Interface Between Fire alarm and Security Panel**



9-6.16.1 Figure 9-2 illustrates the necessary interface signal between the fire alarm system and each local door controller panel. The ESS design needs to include the elements identified in Figure 9-3 for system interface.

**Figure 9-3. Elements of a Fire Alarm System**

- Wire and conduit from the fire alarm system to the security system. It is required that the power and communication lines not be placed in the same conduit.
- Assignment of fire alarm input/output addresses. The fire alarm system sends a signal (fire alarm system output) to each individual door controller in the event of a fire alarm signal.
- Assignment of security system input/output addresses.
- Termination of the fire alarm/security system interface on the fire alarm system.
- Termination of the fire alarm/security system interface on the security system.
- Programming of the fire alarm system to achieve door unlock signals in the event of a fire alarm signal.
- Programming of the security system to achieve door unlock signals in the event of a fire alarm signal.
- Door access control hardware all needs to be "home run" to a local junction box for ease of troubleshooting and repair.

9-6.17 **Intercom System**. While not a requirement, site-specific factors may require provision of an intercom or similar auxiliary communication system at entry portals (such as motorized gates) to communicate with entering personnel from the Dispatch Center or other location.

9-6.18 **Lighting**. While not an official part of ESS, lighting is an effective part of the overall physical protection design. Lighting should be considered as a countermeasure for protection of each critical asset. Coordination with the electrical/lighting engineer needs to occur for placement of lighting to enhance viewing of CCTV systems, as discussed in Chapter Four.

9-6.18.1 Lighting at guard check-points must be sufficient to clearly allow a guard to verify the picture ID on access badges. Some installations may provide a fixed camera at an automatically operated gate for both surveillance and verification of a visual credential for access. In these cases, lighting must similarly be sufficient to allow accurate verification of the picture ID.

## 9-7 MATERIAL ENTRY CONTROL

9-7.1 Other mandates will dictate specific requirements, but the following are typical considerations for material entry control as it relates to ESS and physical security:

9-7.1.1 Material entry control circulation should be separated from general facility traffic.

9-7.1.2 Loading docks are typically monitored by fixed cameras.

9-7.1.3 Rollup doors are normally monitored by an interior point sensor such as a BMS.

9-7.1.4 Shipping and receiving areas are normally caged or secured with a restricted access scheme, such as a higher card access hierarchy level.

# CHAPTER 10

# MODEL DESIGN APPROACH

## 10-1 INTRODUCTION

10-1.1 Other documents provide guidance or directives on design and construction of DoD facilities**.** This chapter presents a model approach on how to design an ESS. The intent of this chapter is not to set new directives, but rather to communicate a process that works well.

10-1.2 Two principal project approaches are design-bid-build and design-build. The model design process outlined in this chapter is applicable to both approaches.

## 10-2 PROJECT PLANNING

10-2.1 As discussed in Chapter 2, ESS is a portion of the portion of the overall physical security scheme for a facility and should be integrated into the overall physical protection plan.

10-2.2 Balance project funding and project scope. Heightened levels of a security system provide increased resistance to intrusion and attack. Increased security brings increased construction costs and complexity. The more complex the system, the more the cost of operation and maintenance will increase. The level of security elements and security requirements need to be identified and reconciled with project funds early in a project. The design team's challenge is to balance security requirements with life safety, convenience, maintenance, and operational costs.

10-2.3 Locating and obtaining CAD backgrounds for site plans and affected buildings should be an early activity. If possible the CAD backgrounds should be provided after contract award and before the kickoff meeting of a project. This will allow the ESS designer or design-builder to have a more effective kickoff meeting. Early in the design process, the ESS designer should conduct site surveys to verify the accuracy of the existing CAD backgrounds and site conditions.

10-2.4 **Site surveys**. Capacity assessment of existing systems:

10-2.4.1 ACS: how many spare card reader slots are available at what panels?

10-2.4.2 What type of credential is used?

10-2.4.3 Is there badging (issuing new badges) capability?

10-2.4.4 CCTV: how many spare camera ports back at central server?

10-2.4.5 Is archiving capability present?

10-2.4.6 IDS: any expansion capability?

10-2.4.7 Transmission system bandwidth availability.

10-2.5 **Coordination of DTM transmission lines**. For existing and new DTM transmission lines, coordinate with the base communications officer (information technology).

10-2.5.1 Approval of radio frequency emitters by local jurisdiction or Host nations must be considered early in the project.

10-2.6 **Dispatch Center.** Identification of the location of the central monitoring facility (space) for the ESS should be made. If sufficient space does not exist for the current project, the Dispatch Center needs to be identified and a scheme for central monitoring made (i.e. a new command center space is required). A determination of Dispatch Center connectivity (DTM) requirements needs to be made. Connectivity requirements refers to bandwidth and pathway considerations. Additionally, distance issues and availability of points of connection needs to be reviewed. There will be additional project cost if new pathways and connections are required.

10-2.7 **Multi-Organizational Interfaces.** Meetings with end users and facility security specialists need to be held. Additionally, determine facility and security forces operational requirements.

10-2.8 **Space Planning.** The ESS designer must interact early to reserve space requirements in a new building (square footage area) fore ESS components such as equipment racks, consoles, operator stations, and administrative stations.

## 10-3 INITIAL DRAWING PREPARATION

10-3.1 A good start for drawing production is to begin with the drawings identified in Figure 10-1.

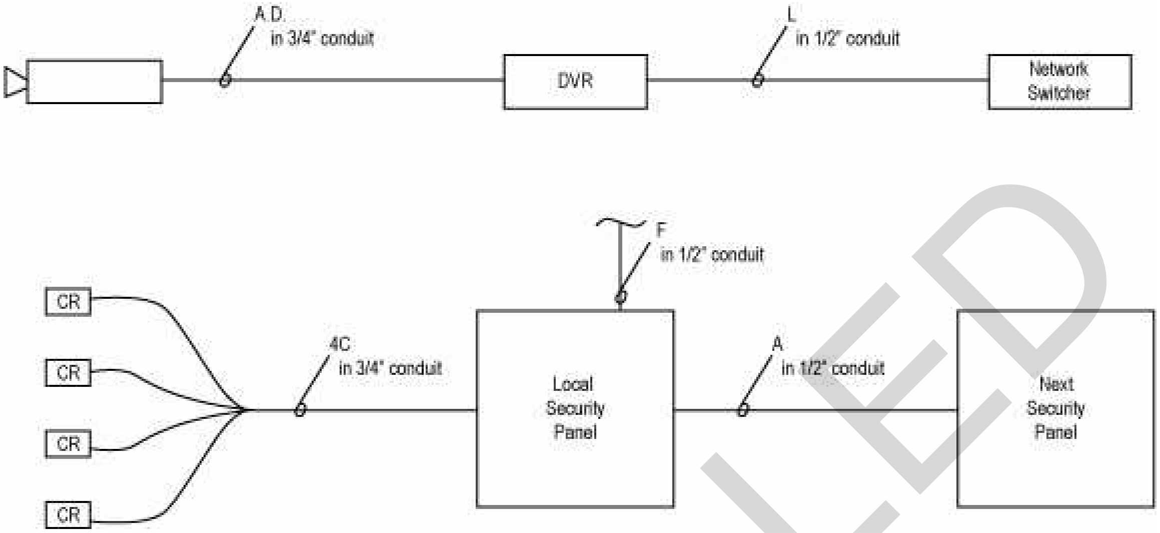
10-3.2 **Cable Schedule.** For identifying different cable types required for a project, a good approach is to use a cable schedule and show the conductor count and cable legend on riser diagrams. A sample is shown in Figure 10-2.

10-3.3 **Functional Matrix.** A document defining the functionality to the system is a useful tool similar to the one shown in Figure 10-3.

## 10-4 BASIS OF DESIGN

10-4.1 Some projects require a Basis of Design. Typically a Basis of Design is done as a report and includes: a functional description of systems, a narrative of systems requirements, some base drawings such as the functional matrix, and documentation of factors effecting the ultimate design and functionality of a system.

## Figure 10-1 Cable Counts on Riser Diagrams



## Figure 10-2. Sample Cable Schedule

| Cable Legend | Style | Type | Use |
|---|---|---|---|
| **A** | #16/1 TSP | Communication Cable<br>Plenum Rated (CMP) | RS-485 |
| **C** | #20 AWG/ 3 TSP | Communications Cable<br>Riser Rated (CMR) | Card reader cable |
| **D** | #20 Coaxial | RG-59U | CCTV Video |
| **E** | #18 Solid /shield | RG-6U | CCTV Video |
| **F** | 2 #12 w/1 #12 ground | THHN | 120 VAC Wiring |
| **G** | #18/1 TP | Communications Cable<br>General Purpose (CMG) | CCTV Video |
| **L** | 8-C | CAT6 | Ethernet cable |
| **U** | 24-strand | 50 micron | Fiber optic cable |
| **W** | ----------- | 50 FT VGA | Workstation to display |

## Figure 10-3. Functional Matrix

| | | Signal sent to security system @ Dispatch Center | DVR records camera image | Guard verifies alarm with camera | UPS system or batteries engage | Local door sounder to alarm | PTZ camera "moves" to preset location | Door unlocks until fire alarm panel is reset | Door unlocks | Motorized gate opens | Response force mobilized |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **ACTION** | A | B | C | D | E | F | G | H | I | J |
| 1 | Valid card reader attempt | ● | | | | | | | ● | | |
| 2 | "Lost card" attempt | ● | ● | ● | | | | | | | |
| 3 | Outdoor microwave sensor alarm | ● | ● | ● | | | ● | | | | |
| 4 | Local security panel power loss | ● | | | ● | | | | | | |
| 5 | Door held open alarm | ● | ● | ● | | ● | ● | | | | |
| 6 | Door forced entry alarm | ● | ● | ● | | ● | ● | | | | |
| 7 | Tamper switch activated on local security panel | ● | | | | | | | | | |
| 8 | Fixed camera video motion detection activated | ● | ● | ● | | | | | | | |
| 9 | Interior motion sensor alarm | ● | | | | | | | | | |
| 10 | Tamper notification activated on security device | ● | | | | | | | | | |
| 11 | Glass break sensor alarm | ● | | | | | | | | | |
| 12 | Fence sensor alarm | ● | ● | ● | | | ● | | | | |
| 13 | Fire panel alarm | ● | | | | | | ● | | | |
| 14 | Remote door access activated | ● | | | | | | | ● | | |
| 15 | Remote gate access activated | ● | ● | | | | | | | ● | |
| 16 | Emergency exit door opened | ● | | | | ● | | | | | |

## 10-5 SCHEMATIC DESIGN PHASE

10-5.1 During schematic design, system solutions for the project issues (problems) identified during programming will be generated. The key product for this phase will be outlined technical specifications and one-line riser diagrams. The schematic design documents can be used to provide the first cost estimate not based on concepts.

10-5.2 Initial panel board schedules should be started to indicate power sources for ESS equipment**.** Any new needs for power panels should be identified by electrical power one-line diagrams.

## 10-6 DESIGN DEVELOPMENT PHASE

10-6.1 During the design development phase, project plans and specifications will be completed. Drawings should include the following:

10-6.1.1 Legends and abbreviations

10-6.1.2 Site plans

10-6.1.3 Floor plans

10-6.1.4 Riser diagrams

10-6.1.5 Mounting details

10-6.1.6 Door hardware schedule (may be on architectural plans)

10-6.1.7 Sequence of construction when applicable

10-6.1.8 Site and floor plans will include power panel locations, security panels, consoles, sensors, cameras, card readers, power circuits, and other related equipment. Riser diagrams should include all devices (including location and zoning requirements), cabling, power connections, grounding, and required system interfaces.

10-6.1.9 The system designer should have owner feedback on any changes to devices upon completion of the design development review meeting.

## 10-7 BIDDING

10-7.1 **Installers and System Integrators.** Installers and integrators must be experienced in the installation, tuning, and programming of ESS. Require a minimum of three years of documented experience for the types of systems the project includes.

## APPENDIX A

## REFERENCES

ASHRAE 62, *Ventilation for Acceptance of Indoor Air Quality*, American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE),

*Design and Evaluation of Physical Protection Systems, The*, 2001, Mary Lynn Garcia, Sandia National Laboratories, Butterworth-Heinemann, Boston

DoD 5200.8, *Physical Security Program*, Department of Defense, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division, http://www.dtic.mil/whs/directives/

DoD 8190.3, *Smart Card Technology,* Department of Defense, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division, http://www.dtic.mil/whs/directives/

DOD 0.2000.12-H, *DoD Antiterrorism Handbook*, Department of Defense, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division, http://www.dtic.mil/whs/directives/

DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, Director of Central Intelligence Directives, http://www.fas.org/irp/offdocs/dcid.htm

*Effective Physical Security*, 3rd Edition, 2004, Lawrence J. Fennelly, Elsevier, Butterworth-Heinemann

FIPS 201, *Standard for Personal Identity Verification of Federal Employees and Contractors*, March 14, 2006, Revision 1, National Institute of Standards and Technology (NIST), 100 Bureau Drive, Stop 1070, Gaithersburg, MD, 20899-1070, http://csrc.nist.gov/piv-program/

GSC-IS V2.1, *Government Smart Card Interoperability Specification*, Version 2.1, 16 July 2003, National Institute of Standards and Technology (NIST), 100 Bureau Drive, Stop 1070, Gaithersburg, MD, 20899-1070, http://smartcard.nist.gov

IES RP-20-98, *Lighting for Parking Facilities*, Illumination Engineering Society of North America (IESNA),

ISO 14443, Part 1, , International Organization for Standardization (ISO), http://www.iso.org

ISO 14443, Part 2

ISO 14443, Part 3,

ISO/IEC 15693-1:2000, *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 1: Physical characteristics*, International Organization for Standardization (ISO), http://www.iso.org

ISO/IEC 15693-2:2000, *Identifications cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 2: Air interface and initialization*, International Organization for Standardization (ISO), http://www.iso.org

ISO/IEC 15693-3:2000, *Identificqation cards - Contactless integrated cicuit(s) cards - Vicinity cards - Part 3: Anticollision and transmission protocol*, International Organization for Standardization (ISO), http://www.iso.org, (available in English only.)

J-STD-607-A, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications (ANSI/J-STD-607-A-2002), 2002, Telecommunication Industry Association (TIA), 2500 Wilson Blvd., Suite 300, Arlington, VA, 22201, http://www.tiaonline.org

MIL-HDBK-1013/1A, *Design Guidance for Physical Security Facilities*, Document Automation and Production Service, Building 4/D, 700 Robbins Ave, Philadelphia, PA, 19111-5094, http://assist.daps.dla.mil/

NFPA 70, *National Electrical Code*, National Fire Protection Association (NFPA), 1 Batterymarch Park, Quincy, MA, 02169-7471, www.nfpa.org

NFPA 101, *Life Safety Code*, National Fire Protection Association (NFPA), 1 Batterymarch Park, Quincy, MA, 02169-7471, www.nfpa.org

NFPA 101B, *Means of Egress for Buildings and Structures*, National Fire Protection Association (NFPA), 1 Batterymarch Park, Quincy, MA, 02169-7471, www.nfpa.org

NFPA 780, *Standard for the Installation of Lightning Protection Systems*, National Fire Protection Association (NFPA), 1 Batterymarch Park, Quincy, MA, 02169-7471, www.nfpa.org

NISTIR 6887, *Government Smart Card Interoperability Specification*, National Institute of Standards and Technology (NIST), 100 Bureau Drive, Stop 1070, Gaithersburg, MD, 20899-1070, http://smartcard.nist.gov

*Perimeter Security Sensor Technologies Handbook*, 1997, Space and Warfare Systems Center, for the Defense Advanced Research Projects Agency Joint Program Steering Group, available at http://www.nlectc.org/perimetr/full2.htm

TIA/EIA 568, *Commercial Building Telecommunications Cabling Standard*, Telecommunication Industry Association (TIA), 2500 Wilson Blvd., Suite 300, Arlington, VA, 22201, http://www.tiaonline.org

TIA/EIA 569, *Commercial Building Standard for Telecommunications Infrastructure of Commercial Buildings*, Telecommunication Industry Association (TIA), 2500 Wilson Blvd., Suite 300, Arlington, VA, 22201, http://www.tiaonline.org

TIA/EIA 606, *Administrative Standard for the Telecommunications Infrastructure of Commercial Buildings*, Telecommunication Industry Association (TIA), 2500 Wilson Blvd., Suite 300, Arlington, VA, 22201, http://www.tiaonline.org

UFC 3-500-10N, *General Electrical Requirements*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

UFC 3-530-01, *Interior and Exterior Lighting and Controls*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

UFC 3-580-10N, *Navy and Marine Corps Intranet (NMCI) Standard Construction Practices*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

UFC 4-010-01, *Minimum Antiterrorism Standards for Buildings*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

UFC 4-010-02, *Minimum Standoff Distances for Buildings (FOUO)*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

UFC 4-012-01, *Security Engineering: Entry Control Facilities/Access Control Points*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

UFC 4-011-01, *DoD Security Engineering Facilities Planning Manual*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

UFC 4-011-02, *DoD Security Engineering Design Manual*, Unified Facilities Criteria Program, Engineering Senior Executive Panel, available from http//dod.wbdg.org

# APPENDIX B

# GLOSSARY

## ACRONYMS AND ABBREVIATIONS

**ACS**—Access control system.

**AA&E**—Arms, ammunition, and explosives.

**BMS**—Balanced magnetic switch.

**BOC**—Base operations center.

**CCD**—Charge-coupled device.

**CAC**—Common access card.

**CCTV**—Closed circuit television system.

**COTS**—Commercial off-the-shelf equipment.

**CPU**—Central processing unit.

**CRT**—Cathode ray tube; commonly used to refer to a computer monitor.

**DBT**—Design basis threat.

**DTM**—Data transmission media.

**DVR**—Digital video recorder.

**EMI**—Electro Magnetic Interference.

**ESS**—Electronic security system.

**ESSC**—Electronic security system console.

**FAR**—False acceptance rate.

**FPR**—False rejection rate.

**FOUO**—For Official Use Only.

**HVAC**—Heating, ventilation, and air conditioning.

**IDE**—Intrusion detection equipment.

**IDS**—Intrusion detection system.

**IP**—Internet protocol.

**IR**—Infrared.

**LAN**—Local Area Network

**LCD**—Liquid crystal display.

**MNS**—Mass notification system.

**NAR**—Nuisance alarm rate.

**NMCI**—Navy/Marine Corps Intranet.

**PCU**—Premise control unit.

**PIN**—Personal identification number.

**PIR**—Passive infrared.

**Pd**—Probability of detection.

**PVC**-Poly-vinyl chloride.

**PTZ**—Pan/tilt/zoom.

**RDTS**—Radar detection system.

**RFID**—Radio frequency identification.

**RDC**—Regional Dispatch Center.

**RMC**—Rigid metal conduit.

**ROC**—Regional Operations Center.

**SCI**—Sensitive compartmented information.

**SCIF**—Sensitive compartmented information facility.

**SEIWG**—Security Equipment Integration Working Group.

**SOC**—Security operations center.

**TDR**—Time Domain Reflectometry.

**UPS**—Uninterruptable power supply.

**VCR**—Video cassette recorder.

**VMD**—Video motion detection.

**WAN**— Wide Area Network

## DEFINITION OF TERMS

**Access Control System (ACS).** An automated system that interfaces with locking mechanisms that momentarily permit access (for example, by unlocking doors or gates) after verifying entry credentials (i.e. using a card reader). Other DoD documents may refer to the ACS as an Automated Access Control System or an Electronic Entry Control system. The ACS may also be referred to as an Automated Access Control System (AACS), Electronic Access Control System, and Electronic Entry Control.

**Arms, Ammunition, and Explosives (AA&E).**

**Balanced Magnetic Switch (BMS)**. A door position switch using a switch held in a balanced or center position by interacting magnetic fields when not in an alarm condition.

**Base Level Information Infrastructure:** That information technology (IT) infrastructure which exists on DoD proprietary or leased property.

**Base Operations Center (BOC).** An operations center for a DoD base, that has equipment and personnel for operational responses. Typically, the BOC is the receiving point for emergency alarms from fire alarm, ESS and 911 calls. This location is typically staffed by trained staff twenty-hour hours a day.. The BOC may have a law enforcement desk of handling domestic dispute or interface with local and federal authorities.. The BOC is typically the will house the Dispatch Center, which is the centralized location for receiving and assessing ESS alarms.

**Cathode Ray Tube (CRT).** A technology used in television and computer display screens. A CRT works by moving an electron beam back and forth across the back of the screen. Each time the beam makes a pass across the screen, it lights up phosphor dots on the inside of the glass tube, thereby illuminating the active portions of the screen. By drawing many such lines from the top to the bottom of the screen, it creates an entire screenful of images.

**Charge-coupled device (CCD)**. A semiconductor technology used to build light-sensitive electronic devices such as cameras and image scanners. Such devices may detect either color or black and white.

**Closed Circuit Television (CCTV) System.** The system that allows video assessment of alarm conditions via remote monitoring and recording of video events.

**Common Access Card (CAC).** As envisioned, the CAC is the standard ID card for DoD personnel. The full implementation of the CAC for access control and personnel information may take three to five years. In addition to providing identification information, it is planned to be the principal card for physical access to buildings and other controlled spaces. It contains limited information related to work function, benefits, and privileges, but does not include medical or personnel records. In addition to allowing building access, it also allows computer logon and enables email encryption and electronic document signatures. The credit card sized CAC uses five different media to store information and enable its different functions: print (digital photograph, hologram, service, grade/rank, expiration date, blood type, donor information, date of birth, and social security number), magnetic stripe and two barcodes (for backward compatibility), and an integrated circuit (IC) chip. The IC chip is the secure portion of the card. It contains all the information stored in the other media on the card, along with certificate, key identifications, and additional pay and medical information. The IC chip can also store additional information and facility-specific needs. The eventual plan is to provide the CAC with wireless, contactless (13.56MHz, compatible with ISO 14443) card reader capability.

**Central Processing Unit (CPU).** In a computer-based system, the component such as a microprocessor, programmable logic controller (PLC), or similar device that functions as the overall system coordinator, performing automated alarm functions, control of peripheral devices, operator interface, alarm reporting, and event logging. CPU is synonymous with the “head-end” of a system and is conceptually the “brains” of the associated system. Contemporary systems use distributed intelligence such that PC functions are downloaded to each local panel, which improves system reliability in the event a communications line is severed.

**Data Transmission Media (DTM).** The system that allows for Electronic Security Systems (ESS) data transmission and communication between system nodes and also back to the Dispatch Center. In other words, the DTM is the security communications system and can consist of dedicated conductors, wireless networks, leased T-1 lines, or virtual private networks. DTM includes both Base Level Information Infrastructure (BLII: on-base) as well as Defense Information Infrastructure (DII: inter-base).

**Defense Information Infrastructure:.** That Information Technology (IT) infrastructure that is not on DoD proprietary or leased property and requires transmission of information across property boundary lines, for example, inter-base communications.

**Dispatch Center.** The space that serves as a central monitoring and assessment facility for the ACS, CCTV, and IDS systems. The key components of a Dispatch Center include consoles, monitors, and printers. Normally, the Dispatch Center is staffed 24 hours a day, seven days a week by trained personnel. Other names for the Dispatch Center include Security Operations Center (SOC), Security Command Center and Security Control Center (SCC), Central Monitoring Station, Data Transmission Center (DTC), and Alarm Control Center (ATC).

**Electronic Security System (ESS).** The integrated electronic system that encompasses interior and exterior Intrusion Detection Systems (IDS), Closed Circuit Television (CCTV) systems for assessment of alarm conditions, Automated Access Control Systems (ACS), Data Transmission Media (DTM), and alarm reporting systems for monitoring, control, and display.

**Electronic Security System Console (ESSC).** While not always specifically referred to as the ESSC, most security systems end up with a console that houses monitoring and server interface equipment**.** Generally, this console is located in the Dispatch Center.

**ElectroMagnetic Interference (EMI).** A naturally occurring phenomena when the electromagnetic field of one device disrupts, impedes, or degrades the electromagnetic field of another device by coming into proximity with it. With ESS, devices are susceptible to EMI because electromagnetic fields are a byproduct of the passing electricity through a wire. Data lines that have not been properly shielded are susceptible to EMI. A good example of an ESS application is using shielded wiring from a field card reader back to the local ACS panel.

**False Acceptance Rate – (FAR).** The rate or percentage at which a false credential is inaccurately accepted as being valid by an ACS. A sample FAR for a product could be 0.1%.

**False Alarm**. An alarm when there is no alarm stimulus.

**False Rejection Rate (FRR).** The rate or percentage at which an ACS product or system rejects an authorized credential holder.

**Frame Rate Per Second (FPS).** When referring to CCTV video image, this term refers to how often the visual still image is being updated. Most movies at the cinema operate at thirty fps. Recommended values for alarm and non-alarm CCTV video fps are provided in the CCTV technical section of the document.

**Intrusion Detection System (IDS).** A system consisting of interior and exterior sensors, surveillance devices, and associated communication subsystems that collectively detect an intrusion of a specified site, facility, or perimeter and annunciate an alarm.

**Local Area Network (LAN).** A geographically limited data communication system for a specific user group consisting of a group of interconnected computers sharing applications, data and peripherals.

**Liquid Crystal Display (LCD).** A type of display used for ESS monitors and other applications. LCDs utilize two sheets of polarizing material with a liquid crystal solution between them. An electric current passes through the crystals to align so that light cannot pass through them. Each crystal, therefore, is like a shutter, either allowing light to pass through or blocking the light. LCD displays can be monochrome or color. Monochrome displays are typically blue or dark gray images on top of a grayish-white background.

**Multiplexing (MUXing).** Combining two or more information channels into a common transmission/storage medium. With old VHS tape systems, the term referred to the storage of four different CCTV camera recordings onto a single VHS tape. With current technology, it is sometimes used to refer to transmission media. For example, a bigger transmission line can be used to bring back six door contact signals from a remote site to a centralized facility on one line as opposed to six different lines. The end result of multiplexing on transmission media is construction cost savings of installing less conductors.

**Nuisance Alarm.** An alarm resulting from the detection of an appropriate alarm stimulus, or failure to use established entry control procedures, but which does not represent an attempt to intrude into the protected area. Examples of nuisance alarms would be an improper opening of a monitored exit door or activation of an exterior intrusion detection system by a DoD maintenance crew. Animal activation of detection systems is a potential cause of nuisance alarms. Another example would be a wind-generated alarm of a fence monitoring system caused by flexing of the fence (which can be compensated for by a wind anemometer). Numerous nuisance alarms can cause complacency.

**Personal Identification Number (PIN).** An identification string used as a password to authenticate identity and gain access to a location or computer resource. Although there are alphanumeric product options, most hardware entry devices make use of a numeric keypad. Many computer resource programs require an alphanumeric string.

**Physical Protection System, Physical Security System.** Means of preventing unauthorized physical access to a system, such as fences, walls, locks, sensors, surveillance, and so on.

**Premise Control Unit (PCU).** A PCU is a specific term defined by DCID 6/9, used to describe the CPU or local security panel for a SCIF. Per the DCID 6/9 definition: the PCU receives signals from all associated sensors in the SCIF’s alarmed zone and establishes the alarm status. The alarm status is immediately transmitted to the monitoring station. Within the monitoring station, a dedicated alarm-monitoring panel (or central processor) monitors incoming PCU signals. On receiving an alarm signal, a monitoring station’s enunciator generates an audible or visual alarm for the monitoring personnel.

**Probability of Detection (Pd)**. A measure of an intrusion detection sensor’s performance in detecting an intruder within its detection zone.

**Proprietary Security Network.** A completely self contained dedicated local area network (LAN) with security system software installed and run on a host server (computer). Proprietary Security Networks are dedicated to the ESS with no outside (Internet, LAN, or WAN) connections.

**Regional Dispatch Center (RDC).** A centralized security command center for multiple bases and facilities within a geographic region. This location is typically staffed twenty-four hours a day by staff trained to assess and initiate response for ESS alarms. The RDC requires interface and communication systems to different bases and facilities. The RDC concept is a trend of economically consolidating different base ESS at one centralized location to save money and infrastructure of having different discrete base operations center.

**Security Equipment Integration Working Group (SEIWG).** A working group responsible for a standard (SEIWG-012) pertaining to information encoded on an access control card. This standard is generally referred to as “SEIWG,” although there are other SEIWG specifications as well. Originally designed by the DoD, the standard’s intent was to provide requirements for an access card that could store enough data to determine information such as the individual cardholder, from which branch of the military the card was issued, and from which base the card was issued, all within the available 40 digits of data storage. The DoD's specification for the CAC is based on the SEIWG standard. To meet the SEIWG standard, three important issues beyond the card and reader must also be addressed:

- The access control software must address the complete SEIWG specification.
- The field panel must handle the 40 digits information resident to the CAC.
- The communication between the card reader and the field panel must be secure.

**Sensitive Compartmented Information (SCI).** Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of Central Intelligence.

**Sensitive Compartmented Information Facility (SCIF).** A facility capable of storing Sensitive Compartmented Information (SCI) material. Requirements for these facilities are defined in Director of Central Intelligence Directive 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*.

**Time Domain Reflectometry (TDR).** Use of sending an electronic signal down a conductor (wiring or cabling) and measuring the time it takes for the signal or part of the signal to return to determine the location of a conductor flaw or disturbance. The signal's reflection begins at the flaw or disturbance point. Once the signal returns, time is converted to distance, then divided by the speed of light, multiplied by the proper velocity of propagation, and the result in divided by two. As used in Intrusion Detection Systems, it is a technology for a fence mounted system that detects intruders climbing or flexing the fence fabric (and thereby inducing a conductor flaw).

**Uninterruptible Power Supply (UPS).** A power supply system that includes a rectifier, battery, and inverter to maintain power in the event of a power outage. UPS systems are specified by hours of operation to sustain power during an outage (six hours, ten hours, or twenty-four hours). UPS systems can be standby power systems or on-line systems. Typically, a centralized UPS is not a mandated requirement for an ESS project.

**Wide Area Network (WAN).** An internetwork that uses telecommunication links to connect geographically distant networks.

Acknowledgement: A computer dictionary called "Webopedia" was used for some of the definitions used in this glossary. Webopedia is found at http://webopedia.com/.