

UNIFIED FACILITIES CRITERIA (UFC)

ELECTRONIC SECURITY SYSTEMS



UNIFIED FACILITIES CRITERIA (UFC)

ELECTRONIC SECURITY SYSTEMS

Any copyrighted material included in this UFC is identified at its point of use. Use of the copyrighted material apart from this UFC must have the permission of the copyright holder.

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER CENTER

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

Change No.	Date	Location
1	09/11/2019	<u>3.4.6 Deleted unsupported Card technologies</u> <u>Appendix C: Updated Notional drawings and text for</u> <u>SCIF, Secure Rooms and Magazines</u>

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 most stringent of the UFC, the SOFA, the HNFA, and the BIA, as applicable.

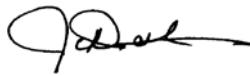
UFC are living documents and will be periodically reviewed, updated, and made available to users as part of the Services' responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC), and Air Force Civil Engineer Center (AFCEC) 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. 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/>.

Refer to UFC 1-200-01, General Building Requirements, for implementation of new issuances on projects.

AUTHORIZED BY:



JAMES C. DALTON, P.E.
Chief, Engineering and Construction
U.S. Army Corps of Engineers



JOSEPH E. GOTT, P.E.
Chief Engineer
Naval Facilities Engineering Command



JOE SCIABICA, SES
Director
Air Force Civil Engineer Center



MICHAEL McANDREW
Director, Facilities Investment and Management
Office of the Deputy Under Secretary of Defense
(Installations and Environment)

**UNIFIED FACILITIES CRITERIA (UFC)
DOCUMENT SUMMARY SHEET**

Document: UFC 4-021-02, *Electronic Security Systems Change 1*

Superseding: UFC 4-012-02, dated 01 October 2013.

Description: This UFC (Unified Facilities Criteria) document provides design requirements and guidance on how to design electronic security systems required by the current antiterrorism/force-protection and physical security 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 Document:

- The design of physical security measures is a specialized technical area that does not fall in the normal skill record and resume of commanders, architects, engineers, and project managers. This document provides guidance to those parties tasked with implementing existing and emerging physical protection system requirements for the protection of DoD assets.

Impact:

- Reduced project costs are achieved by a better understanding of baseline requirements in the specialized technical area of electronic security systems.

Unification Issues

There are no unification issues.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
1-1 PURPOSE	1
1-2 SCOPE	1
1-3 VULNERABILITY AND RISK ASSESSMENT	1
1-4 APPLICABILITY	1
1-5 GENERAL BUILDING REQUIREMENTS	1
1-6 REFERENCES	2
1-7 GLOSSARY	2
1-8 SECURITY ENGINEERING UFC SERIES	2
1-8.1 DoD Minimum Antiterrorism Standards for Buildings	2
1-8.2 DoD Security Engineering Facilities Planning Manual	2
1-8.3 DoD Security Engineering Facilities Design Manual	2
1-8.4 Security Engineering Support Manuals	3
1-8.5 Security Engineering UFC Application	3
CHAPTER 2 ELECTRONIC SECURITY SYSTEM OVERVIEW	5
2-1 OVERVIEW	5
2-2 DETECT, DELAY, AND RESPOND	5
2-2.1 Detect, Delay and Respond Example	5
2-2.2 Alerting a Response Force	8
2-3 ESTABLISH REQUIREMENTS	9
2-3.1 Planning Process	9
2-3.2 Existing Facilities	10
2-4 SYSTEM COMPLEXITY	10
2-4.1 General	10
2-4.2 Simple System	10
2-4.3 Intermediate System	10
2-4.4 Complex System	12
2-4.5 Networked System	12
2-5 MONITORING METHODS	14
2-5.1 General	14
2-5.2 Proprietary Station	14

2-5.3	Local Alarm.....	14
2-5.4	Central Station.....	15
2-5.5	Police Connection.....	15
2-5.6	Summary.	16
CHAPTER 3 ACCESS CONTROL SYSTEMS		17
3-1	OVERVIEW.	17
3-1.1	Elements.....	17
3-1.2	Methodology.	17
3-2	ACS ENTRY-AUTHORIZATION IDENTIFIERS.....	17
3-2.1	Credential Devices.....	19
3-2.2	Coded Devices.	19
3-2.3	Biometric Devices.....	20
3-2.4	Combining Entry Authorization Identifiers.....	21
3-2.5	Selecting Entry Authorization Identifiers.....	21
3-3	OTHER ACS FEATURES.....	22
3-3.1	Anti-Passback.....	22
3-3.2	Anti-Tailgating.....	22
3-3.3	Two-Man Rule.	22
3-3.4	Event Tracking/Event Logs.....	23
3-4	ACS EQUIPMENT.....	23
3-4.1	Badging Equipment.	23
3-4.2	ACS Central Computer.....	24
3-4.3	ACS Workstation.	24
3-4.4	ACS Local Processor.....	24
3-4.5	Card Readers.	24
3-4.6	Card Types.	25
3-4.7	Keypads and PIN Codes.....	27
3-4.8	Biometric Readers.	27
3-4.9	Request-to-Exit (REX) Devices.....	29
3-5	ACS DESIGN CONSIDERATIONS.....	30
CHAPTER 4 CLOSED CIRCUIT TELEVISION SYSTEMS		33
4-1	OVERVIEW.....	33

4-1.1	Alarm Assessment.....	33
4-1.2	Access Control.....	33
4-1.3	Surveillance.....	33
4-1.4	Evidentiary Archives.....	33
4-2	CAMERAS.....	34
4-2.1	Color Versus Black and White.....	34
4-2.2	Indoor Cameras.....	35
4-2.3	Outdoor Cameras.....	35
4-2.4	Fixed Position Cameras.....	36
4-2.5	Pan/Tilt/Zoom (PTZ) Cameras.....	36
4-2.6	Dome Cameras.....	37
4-2.7	IP and Analog Cameras.....	37
4-3	ILLUMINATION.....	38
4-3.1	Illuminance.....	38
4-3.2	Uniformity.....	38
4-3.3	Glare Reduction.....	41
4-3.4	Interior Lighting.....	41
4-4	VIEWING IN LOW-LIGHT CONDITIONS.....	42
4-4.1	Black/White Switching.....	42
4-4.2	Infrared Illuminators.....	42
4-4.3	Thermal Imagers.....	43
4-5	ANGLE OF VIEW AND FIELD OF VIEW.....	43
4-6	CAMERA RESOLUTION.....	46
4-7	VIDEO FRAME RATE.....	48
4-8	DIGITAL VIDEO BANDWIDTH.....	49
4-9	DIGITAL VIDEO RECORDING.....	50
4-9.1	Memory Card.....	50
4-9.2	Digital Video Recorder (DVR).....	50
4-9.3	Network Video Recorder (NVR).....	50
4-9.4	Hybrid Video Recorder (HVR).....	51
4-9.5	Required Storage Capacity.....	51
4-10	CCTV WORKSTATION.....	52

4-11	VIDEO ANALYTICS.....	52
4-12	CCTV DESIGN PROCESS SUMMARY.	53
4-12.1	Define Security Objectives for the CCTV System.....	53
4-12.2	Develop a Camera Layout to Meet the Security Objectives.....	53
4-12.3	Verify That Illumination Is Sufficient For Each Scene Of Interest.....	53
4-12.4	Specify Workstation Locations.....	53
4-12.5	Specify Recording Locations and Capacity.....	53
4-12.6	Define Network Architecture.	53
4-12.7	Define Power Requirements.....	53
4-12.8	Describe Software and Integration Requirements.	54
CHAPTER 5	INTRUSION DETECTION SYSTEM.....	55
5-1	OVERVIEW.	55
5-2	SYSTEM CONFIGURATION.....	55
5-2.1	Policy Compliance.	55
5-2.2	Alarm Monitoring Location(s).....	55
5-2.3	Zone Definition.....	57
5-2.4	IDS/ACS Integration.	57
5-3	INTERIOR SENSORS.....	59
5-3.1	Interior Point Sensors.	59
5-3.2	Interior Volumetric Sensors.....	61
5-3.3	Acoustic Sensors.	61
5-3.4	Passive Infrared (PIR) Sensors.	61
5-3.5	Ultrasonic Sensors.....	62
5-3.6	Dual-Technology Sensors.....	62
5-4	EXTERIOR SENSORS.....	63
5-4.1	Open Terrain.....	63
5-4.2	Property/Fence Line Detection.	68
5-4.3	Other Exterior Sensors.	70
5-4.4	Double Fence Concept.	71
5-4.5	False Alarm Causes for Exterior Sensors.....	71
5-5	VIDEO ANALYTICS FOR IDS.....	72
5-6	“AND/OR” CONFIGURATION OPTIONS.....	72

5-7	IDS DESIGN GUIDANCE.....	73
5-7.1	Critical Asset Case Study.....	73
5-7.2	Additional IDS Design Guidance.....	75
5-8	SUMMARY.....	76
CHAPTER 6 DATA TRANSMISSION MEDIA (DTM).....		77
6-1	INTRODUCTION.....	77
6-2	BANDWIDTH ANALYSIS.....	77
6-3	SECURE COMMUNICATIONS.....	77
6-4	NETWORK TOPOLOGY.....	77
6-4.1	General Network Topologies.....	78
6-5	COMMUNICATION REDUNDANCY.....	81
6-6	TRANSMISSION MODES/PROTOCOLS.....	82
6-7	TRANSMISSION MEDIA.....	82
6-7.1	Hardwired.....	82
6-7.2	Direct Subscriber Lines (T 1 Lines).....	83
6-7.3	Wireless.....	83
6-7.4	Free-Space Optics (FSO).....	83
6-8	TECHNOLOGY COMPARISION.....	85
6-9	ENCRYPTION.....	85
CHAPTER 7 DISPATCH CENTER.....		87
7-1	INTRODUCTION.....	87
7-1.1	Dispatch Center.....	87
7-1.2	Regional Dispatch Center (RDC).....	87
7-1.3	Small Facility Options.....	88
7-2	SPACE.....	88
7-2.1	Space Programming.....	88
7-3	LIGHTING.....	89
7-4	CONSOLES.....	89
7-5	MONITORS.....	89
7-6	GROUNDING/POWER CONDITIONING.....	90
7-7	HEATING, VENTILATION AND AIR CONDITIONING.....	90
7-7.1	Environmental Considerations.....	90

7-7.2	Load Calculation Considerations.	91
7-7.3	Components Considerations.....	91
7-8	SUPPORT ROOMS.....	91
CHAPTER 8 ESS SUBSYSTEM INTEGRATION.....		93
8-1	OVERVIEW.	93
8-2	COMMUNICATION FROM THE IDS TO THE ACS.	93
8-3	COMMUNICATION FROM THE IDS TO THE CCTV SYSTEM.	93
8-3.1	Hardwired Conductors.....	93
8-3.2	Serial Communications.....	94
8-3.3	Software-Based Integration for Networked ESS.....	94
8-4	COMMUNICATION FROM THE CCTV SYSTEM TO THE ACS.....	94
8-5	COMMUNICATION FROM THE ACS TO THE DISPATCH CENTER. ...	94
8-6	DESIGN GUIDANCE ON IT SYSTEM COORDINATION.....	95
CHAPTER 9 GENERAL CONSIDERATIONS AND CROSS-DISCIPLINE		
COORDINATION.....		97
9-1	GENERAL CONSIDERATIONS.....	97
9-1.1	General.....	97
9-1.2	System Acceptance Testing.	97
9-1.3	Operation and Maintenance.....	98
9-2	GENERAL COORDINATION.	98
9-3	CIVIL COORDINATION.....	98
9-3.1	Gate Control (Vehicle Gates and Sally Ports).....	98
9-3.2	Underground Site Work.	99
9-3.3	Outdoor Perimeter Security Features.	99
9-4	ARCHITECTURAL COORDINATION.	99
9-4.1	Balance of Security with Convenience.....	99
9-5	LIFE SAFETY CODE COORDINATION.....	102
9-6	ELECTRICAL COORDINATION.	102
9-6.1	Power.....	102
9-6.2	Backup Power.....	102
9-6.3	Grounding, Bonding, and Lightning Protection.	103
9-6.4	Cable Type.	103
9-6.5	Surge Protection.	103

9-6.6	Electromagnetic Interference (EMI).....	103
9-6.7	Tamper Protection.....	103
9-6.8	Radio Frequencies.....	105
9-6.9	Voltage Drop Considerations.....	105
9-6.10	Harmonics.....	105
9-6.11	Raceway.....	106
9-6.12	Labeling.....	106
9-6.13	Shielding.....	106
9-6.14	Fire Alarm System.....	106
9-6.15	Intercom System.....	107
9-6.16	Lighting.....	107
9-7	MATERIAL ENTRY CONTROL.....	108
CHAPTER 10 MODEL DESIGN APPROACH.....		109
10-1	INTRODUCTION.....	109
10-2	PROJECT PLANNING.....	109
10-2.1	Balance Project Funding and Project Scope.....	109
10-2.2	Existing Site and Building Plans.....	109
10-2.3	Site Surveys.....	109
10-2.4	Dispatch Center.....	110
10-2.5	Multi-Organizational Interfaces.....	110
10-2.6	Space Planning.....	110
10-3	INITIAL DRAWING PREPARATION.....	110
10-3.1	Cable Schedule.....	110
10-3.2	Functional Matrix.....	111
10-4	BASIS OF DESIGN.....	111
10-5	SCHEMATIC DESIGN PHASE.....	112
10-6	DESIGN DEVELOPMENT PHASE.....	113
10-7	BIDDING.....	113
APPENDIX A REFERENCES.....		115
APPENDIX B GLOSSARY.....		120
B-1	ACRONYMS AND ABBREVIATIONS.....	120
B-2	DEFINITION OF TERMS.....	122

APPENDIX C NOTIONAL INTERIOR IDS CONFIGURATIONS	128
C-1 SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF)..	128
C-1.1 DoD Criteria Document.....	128
C-1.2 Policy Baseline.	128
C-1.3 Baseline Intrusion Detection System (IDS) Requirements.....	129
C-1.4 Cameras.	129
C-1.5 Tamper Protection.	129
C-1.6 External Transmission Line Security.....	130
C-1.7 Emergency Backup Electrical Power.	130
C-1.8 Optional Equipment.	130
C-2 SECURE ROOM (TOP SECRET OR SECRET OPEN STORAGE).....	131
C-2.1 Policy Baseline.	131
C-2.2 Baseline Intrusion Detection System (IDS) Requirements.....	131
C-2.3 Cameras.	132
C-2.4 Tamper Protection.	132
C-2.5 External Transmission Line Security.....	132
C-2.6 Emergency Backup Electrical Power.	132
C-3 ARMS STORAGE AREA (ARMORY, ARMS ROOM, READY ISSUE ROOM).....	133
C-3.1 Policy Baseline.	133
C-3.2 Baseline Intrusion Detection System (IDS) Requirements.....	133
C-3.3 Tamper Protection.	134
C-3.4 Emergency Backup Electrical Power.	135
C-4 MAGAZINE.....	135
C-4.1 Policy Baseline.	135
C-4.2 Baseline Intrusion Detection System (IDS) Requirements.....	135
C-4.3 Tamper Protection.	136
C-4.4 Emergency Backup Electrical Power.	136

FIGURES

Figure 1-1 Security Engineering UFC Application.....	4
Figure 2-1. ESS as a Part of a Physical Security System.	6
Figure 2-2. Example Detect and Delay Options.	7

Figure 2-3. Timeline Showing Two Cases of Breach and Detection.	9
Figure 2-4. Project Process.....	11
Figure 2-5. Intermediate System with Separate ACS and IDS.....	12
Figure 2-6. Complex System With Separate ACS, IDS, and CCTV Subsystems.....	12
Figure 2-7. Networked System.....	13
Figure 2-8. Proprietary Station Monitoring.....	14
Figure 2-9. Local Alarm Monitoring.....	15
Figure 2-10. Central Station Monitoring.....	15
Figure 2-11. Police Connection Monitoring.....	16
Figure 3-1. Example Access Control System (ACS).....	18
Figure 3-2. Advantages and Disadvantages of Using Credential Devices.....	19
Figure 3-3. Advantages and Disadvantages of Using Coded Devices.....	20
Figure 3-4. Advantages and Disadvantages of Using Biometric Devices.....	21
Figure 3-5. Sample Card Reader Door Configuration.....	26
Figure 3-6. ACS Design Process.....	32
Figure 4-1. Example Block Diagram for a Networked CCTV System.....	34
Figure 4-2. Scene Illuminance and Faceplate Illuminance.....	40
Figure 4-3. Effect of Glare on CCTV Camera Image Quality.....	41
Figure 4-4. Angle of View and Field of View.....	44
Figure 5-1. Example Intrusion Detection System (IDS).....	56
Figure 5-2. Example Exterior IDS Zone Layout.....	58
Figure 5-3. Separate ACS and IDS.....	58
Figure 5-4. Sample Door Configuration.....	59
Figure 5-5. Sample Window Configuration.....	60
Figure 5-6. Sample Roof Hatch Configuration.....	60
Figure 5-7. Active Infrared IDS.....	64
Figure 5-8. Monostatic Microwave Sensor and Associated Footprints.....	65
Figure 5-9. Bistatic Microwave Sensor Operation.....	66
Figure 5-10. Typical Bistatic Microwave Layout and Guidance.....	67
Figure 5-11. Typical Fiber Optic Fence Detection System.....	69
Figure 5-12. Double Fence Example.....	71
Figure 5-13. Zoned Detection System.....	74
Figure 6-1 Star Topologies.....	79
Figure 6-2. Ring Topologies.....	80
Figure 6-3. Fully-Meshed Topologies.....	81
Figure 7-1. Dispatch Center Centrally Located.....	87
Figure 7-2. Example RDC.....	88
Figure 7-3. Sample Simple Dispatch Center Console Layout.....	89
Figure 7-4. Sample Small-Medium Dispatch Center Space Layout.....	90
Figure 9-1. Elements of a Fire Alarm System.....	107
Figure 10-1 Cable Counts on Riser Diagrams.....	111
Figure 10-2. Sample Cable Schedule.....	111
Figure 10-3. Functional Matrix.....	112

TABLES

Table 2-1. Example Breach Events and Delay Time.....	7
Table 2-2. Sample Detect, Delay, and Respond Measures.....	7
Table 2-3 Pros and Cons of Monitoring Methods.....	16
Table 4-1. Fixed versus PTZ Cameras.....	37
Table 4-2. Reflectivity Factors for Various Surface Conditions.....	40
Table 4-3. Characteristics of Thermal Imagers.....	43
Table 4-4. Typical Faceplate Sizes.....	46
Table 4-5. Typical Camera Resolution Specifications.....	46
Table 4-6. Object Discrimination Levels Based on Johnson Criteria.....	47
Table 4-7. Single-frame File Size for Various Resolution Values and Compression Schemes.....	50
Table 5-1. Application Notes – Interior IDS Sensors.....	63
Table 5-2. False Alarm Causes—Exterior IDS Sensors.....	71
Table 5-3. Advantages and Disadvantages of “AND” and “OR” Configurations.....	73
Table 5-4. Sample Probability of Detection Factors.....	73
Table 5-5. IDS Design Guidance.....	75
Table 5-6. Exterior IDS Applications Table.....	75
Table 6-1. Bandwidth Usage Values.....	78
Table 6-2. Data Transmission.....	84
Table 6-3. DTM Technologies for ESS.....	86

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 SCOPE.

This UFC provides design requirements and guidance for the design of 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 policy, service policy, installation requirements, or user requirements. Projects may include new construction, additions, renovations, expeditionary, or temporary construction.

1-3 VULNERABILITY AND RISK ASSESSMENT.

In accordance with DOD O-2000.12H Antiterrorism handbook, a vulnerability and risk assessment must be conducted prior to beginning any security project. Upon identifying facility or asset vulnerabilities to threats, physical security measures such as ESS may be deployed to reduce vulnerabilities. In summary, this document assumes the pre-design phases, including the risk analysis, are complete prior to beginning design. For information on Security Engineering Planning and Design process, refer to UFC 4-020-01 and UFC 4-020-02 (described in the section "Security Engineering UFC Series" in this chapter). The engineering risk analysis conducted as part of UFC 4-020-01 should be consistent with the terrorism risk analysis conducted by the installation security/AT staff.

1-4 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.

1-5 GENERAL BUILDING REQUIREMENTS.

UFC 1-200-01, "General Building Requirements", provides applicability of model building codes and government-unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, sustainability, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

1-6 REFERENCES.

Appendix A contains a list of references used in this document. The publication date of the code or standard is not included in this document. The most recent edition of referenced publications applies, unless otherwise specified.

1-7 GLOSSARY.

Appendix B contains acronyms, abbreviations, and terms.

1-8 SECURITY ENGINEERING UFC SERIES.

This UFC is one of a series of security engineering unified facilities criteria documents that cover minimum standards, planning, preliminary design, and detailed design for security and antiterrorism. The manuals in this series are designed for a diverse audience to facilitate development of projects throughout the design cycle. The manuals in this series include: the following:

1-8.1 DoD Minimum Antiterrorism Standards for Buildings.

UFC 4-010-01 and UFC 4-010-02 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.

1-8.2 DoD Security Engineering Facilities Planning Manual.

UFC 4-020-01 presents processes for developing the design criteria necessary to incorporate security and antiterrorism into DoD facilities and for identifying the cost implications of applying those design criteria. Those design criteria may be limited to the requirements of the minimum standards, or they may include protection of assets other than those addressed in the minimum standards (people), aggressor tactics that are not addressed in the minimum standards or levels of protection beyond those required by the minimum standards. The cost implications for security and antiterrorism are addressed as cost increases over conventional construction for common construction types. The changes in construction represented by those cost increases are tabulated for reference, but they represent only representative construction that will meet the requirements of the design criteria. The manual also addresses the tradeoffs between cost and risk. The Security Engineering Facilities Planning Manual is intended to be used by planners as well as security and antiterrorism personnel with support from planning team members.

1-8.3 DoD Security Engineering Facilities Design Manual.

UFC 4-020-02 provides interdisciplinary design guidance for developing preliminary systems of protective measures 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 as such can provide a good basis for a more detailed design. The manual also provides a process for assessing the impact of protective measures on risk. The primary audience for the Security Engineering Design Manual is the design team, but it can also be used by security and antiterrorism personnel.

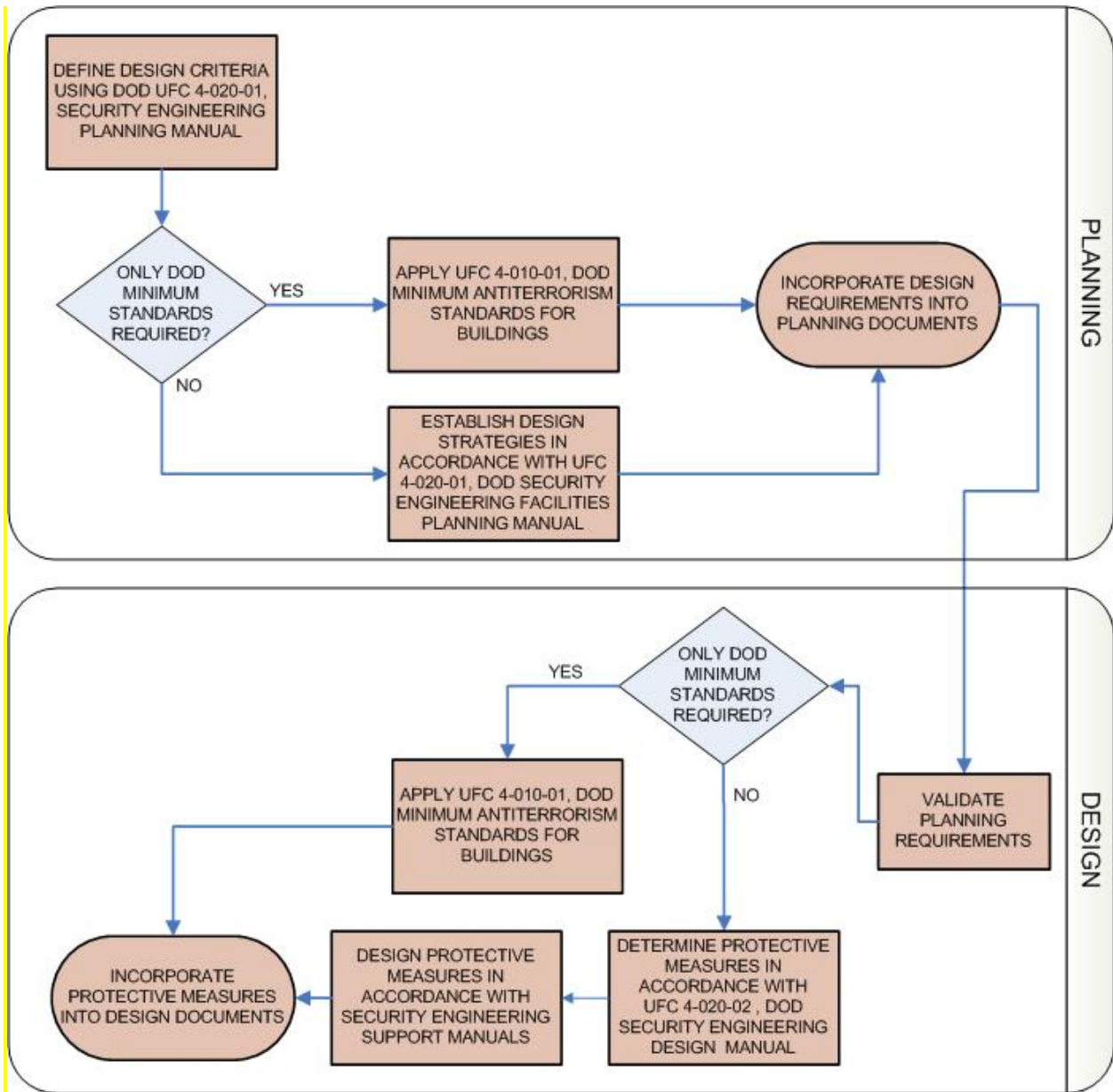
1-8.4 Security Engineering Support Manuals.

In addition to the standards, planning, and design UFCs mentioned above, there is a series of additional UFCs that provide detailed design 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 mail rooms. 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.

1-8.5 Security Engineering UFC Application.

The application of the security engineering series of UFCs is illustrated in Figure 1-1. UFC 4-020-01 is intended to be the starting point for any project that is likely to have security or antiterrorism requirements. By beginning with UFC 4-020-01, the design criteria will be developed that establishes which of the other UFCs in the series will need to be applied. The design criteria may indicate that only the minimum standards need to be incorporated, or it may include additional requirements, resulting in the need for application of additional UFCs. Even if only the minimum standards are required other UFCs may need to be applied if sufficient standoff distances are unavailable. Applying this series of UFCs in the manner illustrated in Figure 1-1 will result in the most efficient use of resources for protecting assets against security and antiterrorism related threats.

Figure 1-1 Security Engineering UFC Application.



CHAPTER 2 ELECTRONIC SECURITY SYSTEM OVERVIEW

2-1 OVERVIEW.

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 and redundancy, 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 4-021-01 for Mass Notification System design guidance.

2-2 DETECT, DELAY, AND RESPOND.

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.)

2-2.1 Detect, Delay and Respond Example.

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 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. 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. Depending on the nature of the asset, there are some dictated response times. The ESS designer should work with the facility/base security officer to identify the response forces and reaction times. Security and planning personnel should refer to DoD, agency, and service directives to identify response requirements.

Detect, Delay, and Respond Factors Samples. 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.

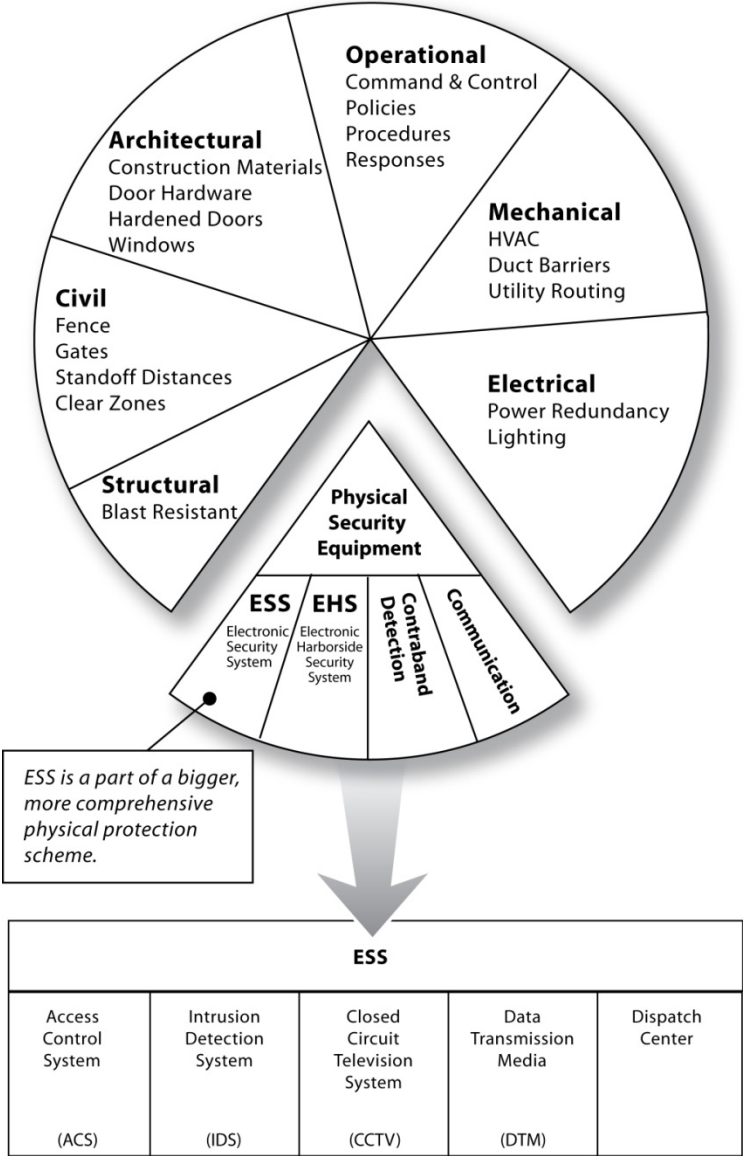


Figure 2-2. Example Detect and Delay Options.

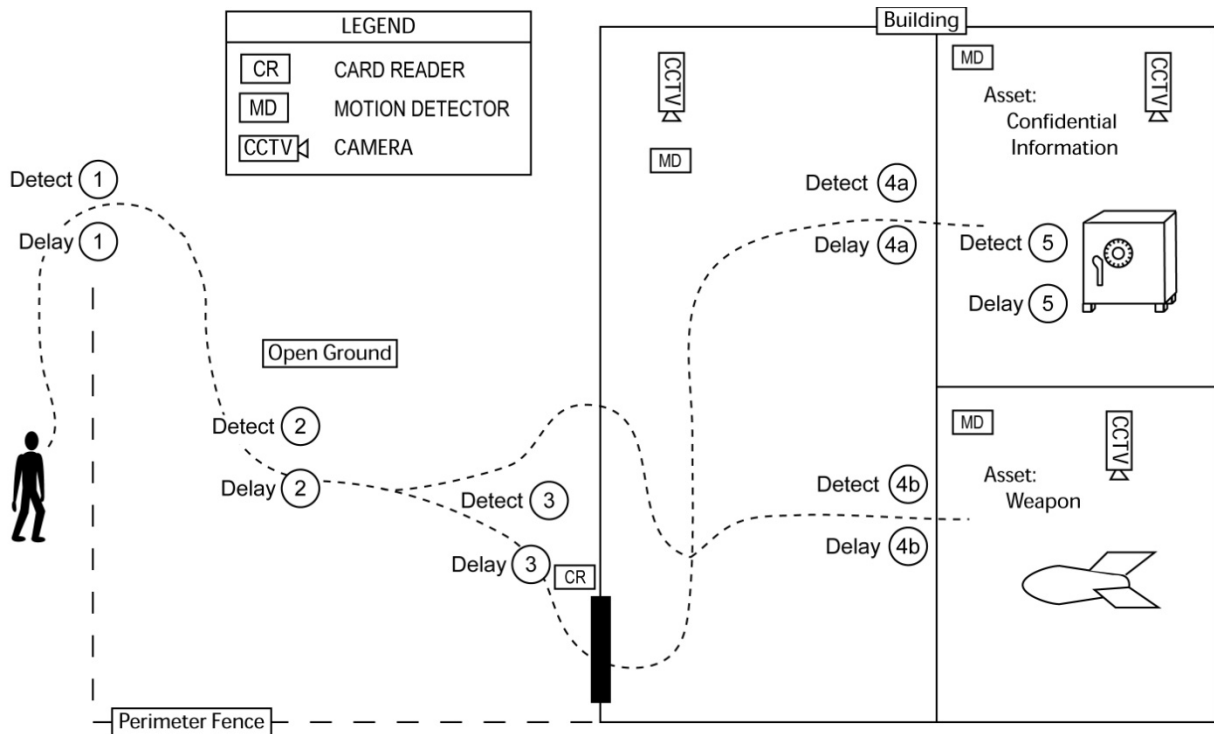


Table 2-1. Example Breach Events and Delay Time.

	Delay Options	Delay Time	Detection Options
1	Climb fence	8-10 sec.	Perimeter fence detection system
2	Cross open ground (for example 600 feet)	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.

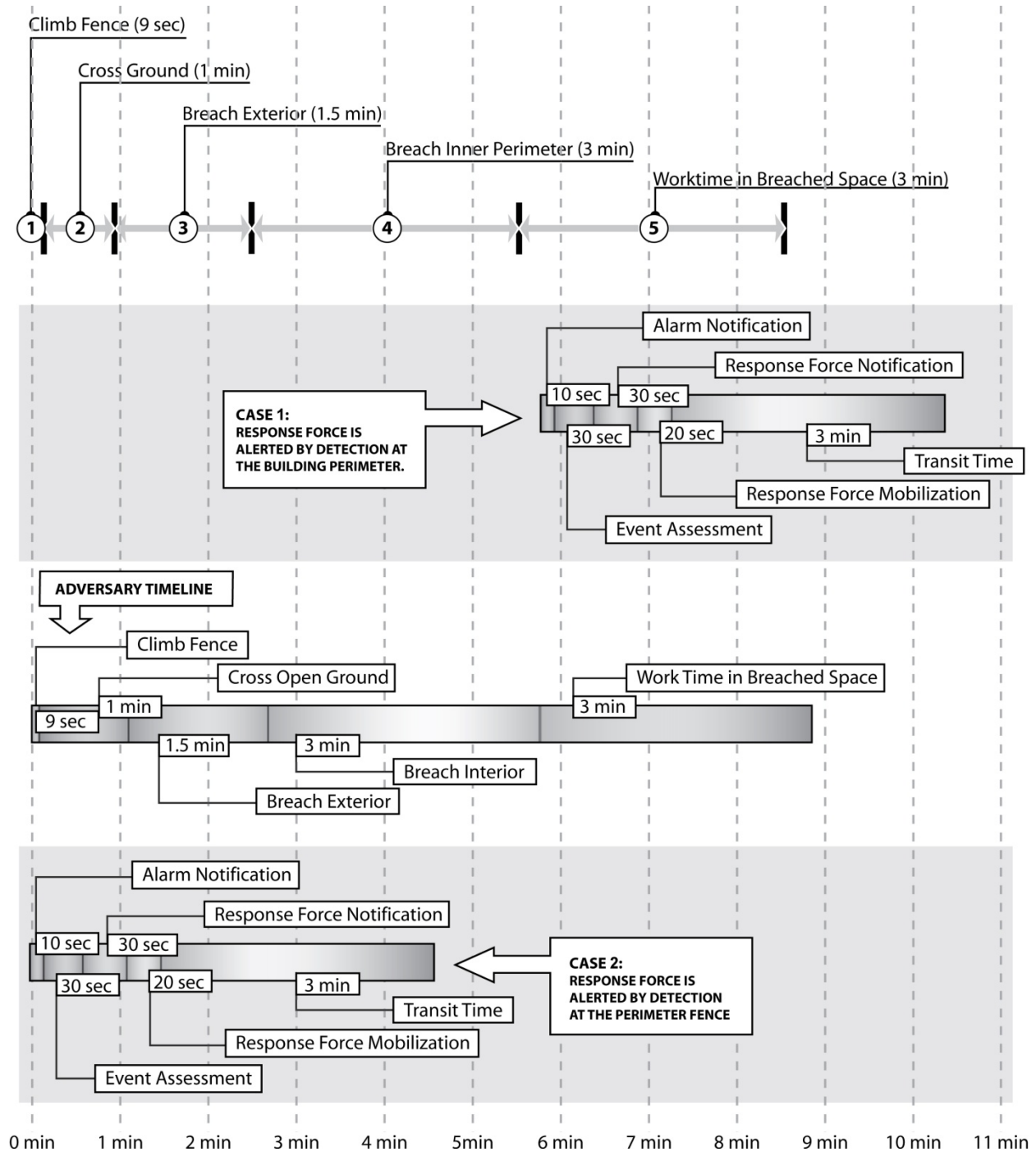
Detect Measures	Delay Measures	Respond Measures
Intrusion detection devices	Fences	Response force alerted
Alarm notification	Walls	Response force travel
Visual displays	Doors	Neutralization

2-2.2 Alerting a Response Force.

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 nearly six minutes after the adversary climbs the perimeter fence, 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, thus allowing response forces to arrive and intervene before the asset is compromised.

The timeline in figure 2-3 illustrates two different security strategies - containment and denial. A containment strategy concedes that the adversary may gain physical access to the protected asset, but it ensures that the response force arrives soon thereafter, thus containing the degree to which the asset is compromised. However, the asset may be damaged or destroyed, depending on the objective and capabilities of the adversary. A denial strategy, on the other hand, ensures that the protected asset is in no way compromised by the adversary. Denial generally requires early detection, long delay, and rapid response to ensure that the adversary is unable to gain physical access to the protected asset.

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



2-3 ESTABLISH REQUIREMENTS.

2-3.1 Planning Process.

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 to determine 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, information assurance, 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.

2-3.2 Existing Facilities.

For existing facilities, the design criteria are 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 are 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 4-020-01 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.

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, an IDS at a low value asset is a simple system. 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).

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. 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. A basic block diagram for this type of system reporting to a common Dispatch Center is shown in Figure 2-5.

Figure 2-4. Project Process.

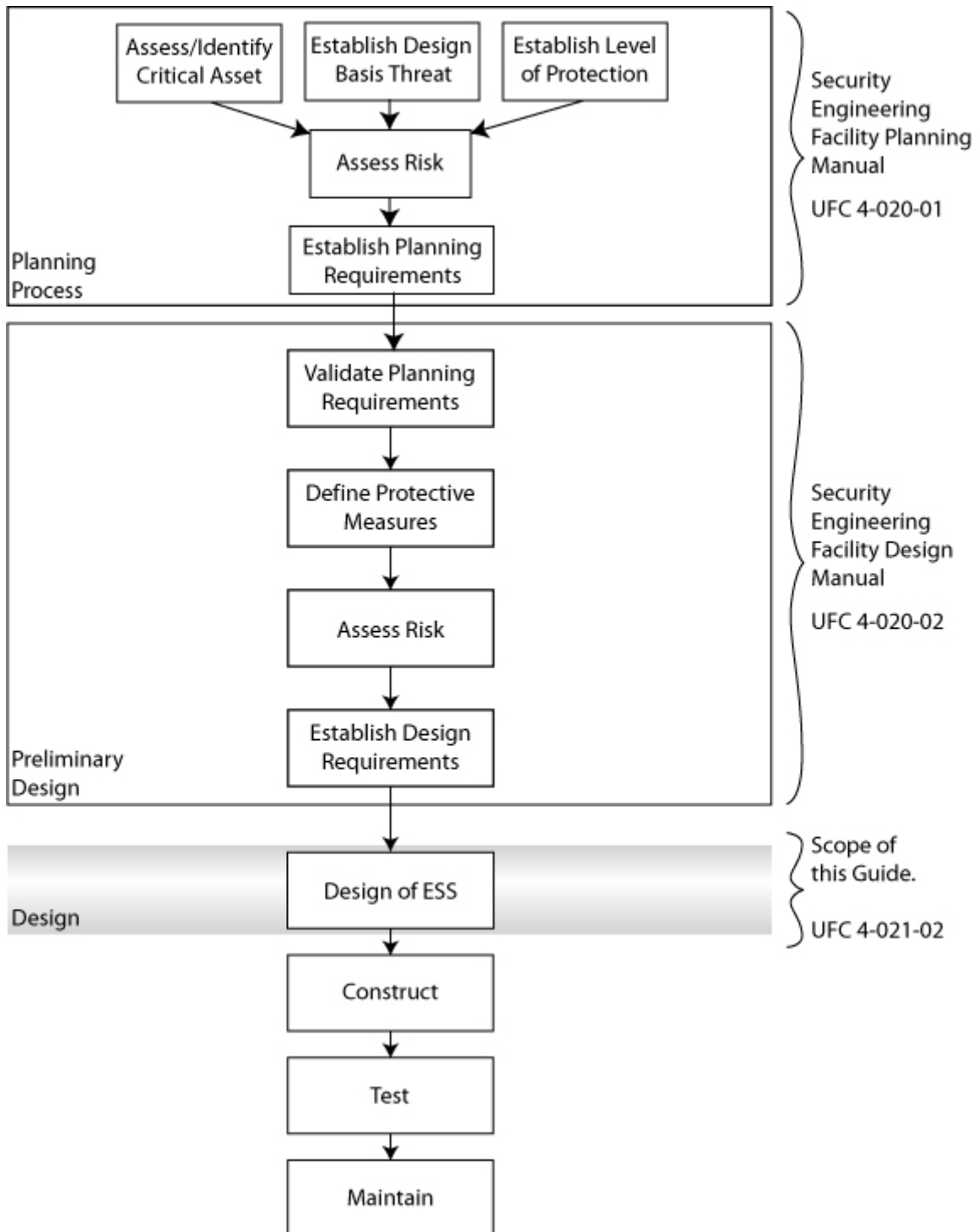
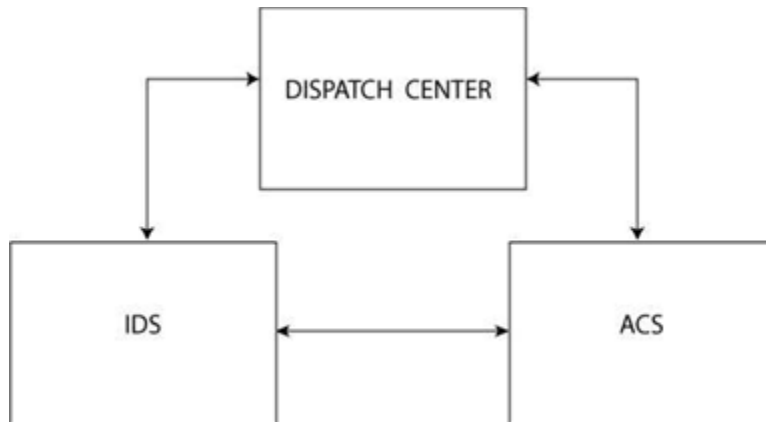


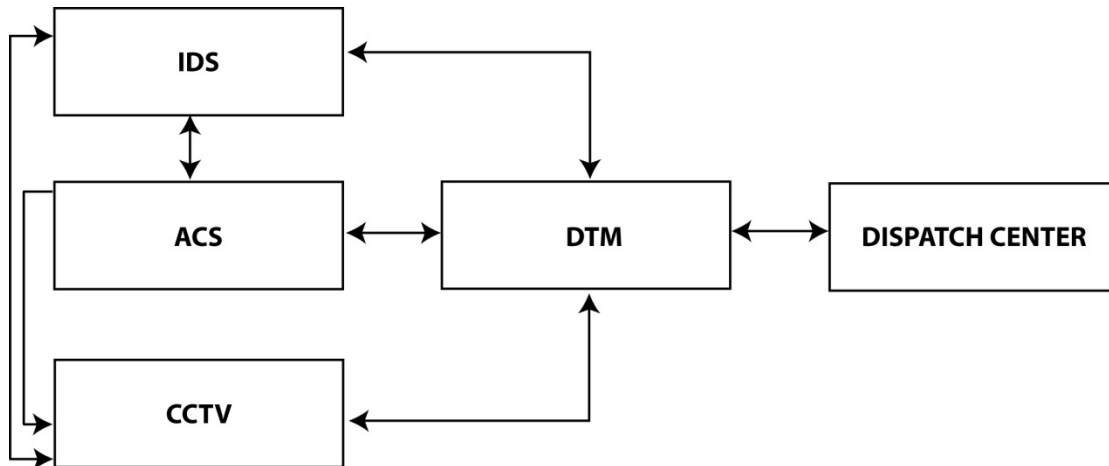
Figure 2-5. Intermediate System with Separate ACS and IDS.



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 2-6.

Figure 2-6. Complex System With Separate ACS, IDS, and CCTV Subsystems.



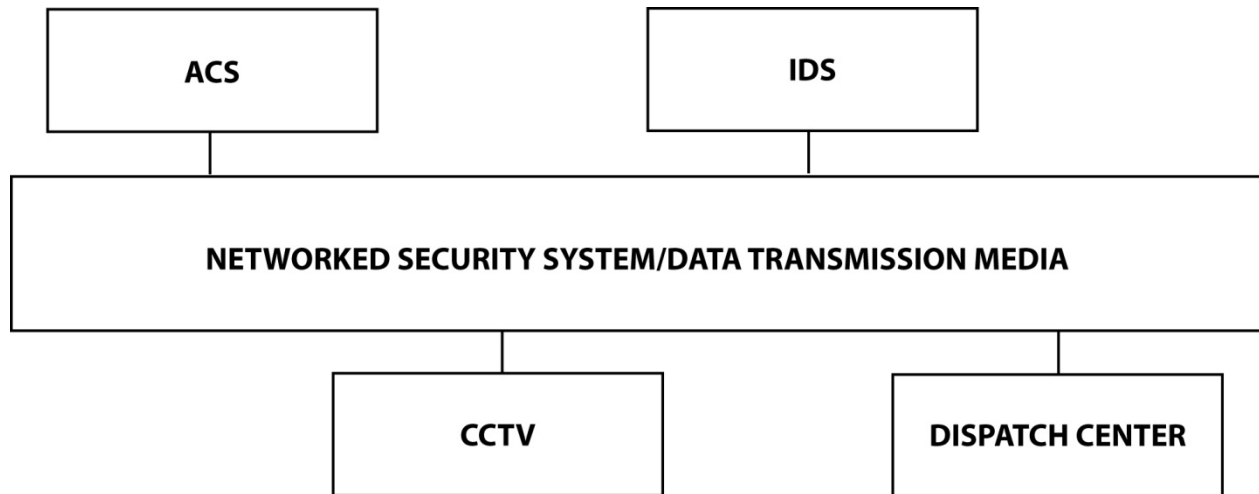
In Figure 2-6, the lines from the ACS/IDS to the CCTV system represent the integration required to automatically display a user-specified camera scene when triggered by a corresponding intrusion or access control alarm. The integration can vary from hardwired contacts to intelligent data communications. System interfaces and integration are described further in Chapter 8, "ESS Subsystem Integration."

2-4.5 Networked System.

The networked security system, illustrated in Figure 2-7, operates on a single network with drivers to the different discrete components of the subsystems. Responding to the proliferation of networks supporting Ethernet and Internet protocols, the security industry now offers many network-ready components such as local processors for ACS

and IDS, intrusion panels, cameras, biometric devices, intercom stations, video recorders, central station receivers, file servers, and workstations. Application software and device drivers are also widely available to allow integration and management of all subsystems across the network. Refer to Chapter 8, "ESS Subsystem Integration" for more information.

Figure 2-7. Networked System.



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 information assurance policies and procedures. For example, the DoD Information Assurance Certification and Accreditation Process (DIACAP) is described in DoDI 8510.01. A unique user ID and password is required for each individual granted access to the 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. The system must monitor and log all network and ESS component access attempts and all changes to ESS applications 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.

2-5 MONITORING METHODS.

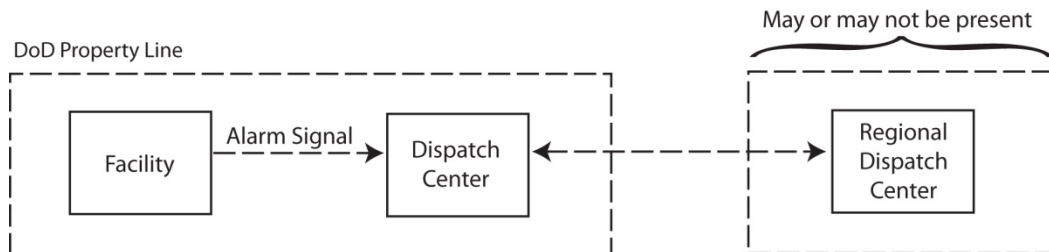
2-5.1 General.

The ESS designer must determine the alarm monitoring method early in the project planning process. This will ensure that issues related to alarm monitoring such as equipment compatibility, data transmission, space allocation, manpower, and standard operating procedures can be adequately addressed in the design phase. Four alarm monitoring methods are defined in DoD 0-2000.12-H - proprietary station, local alarm, central station, and police connection. These methods are described in the following paragraphs.

2-5.2 Proprietary Station.

A proprietary station is a method in which a property owner provides all facilities, equipment, and staffing necessary to monitor alarms. This is the preferred and most common method for a DoD installation where a Dispatch Center functions as a proprietary station and 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 2-8: a Dispatch Center centrally located at a base or a detached Regional Dispatch Center (RDC).

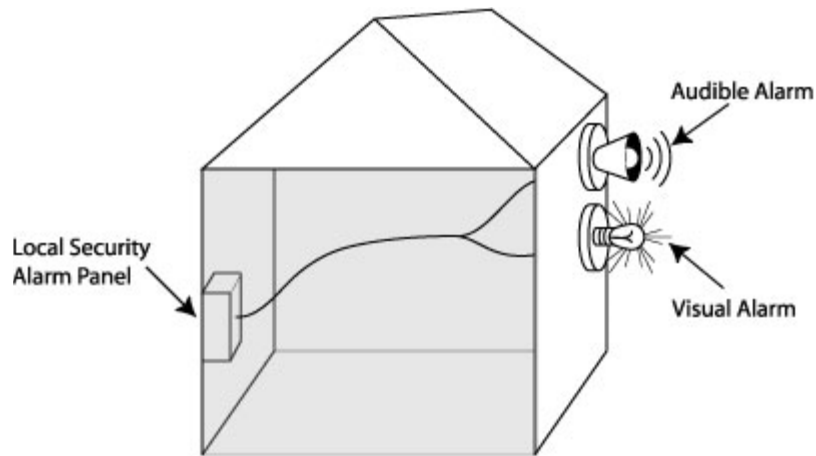
Figure 2-8. Proprietary Station Monitoring.



2-5.3 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, but they cannot be relied upon to initiate the Detect, Delay, Respond sequence. Because of this limitation, a local audible/visible alarm should not be used as the sole means of annunciation. In some cases, however, it may be beneficial to provide a local alarm in addition to annunciation at a qualified monitoring station.

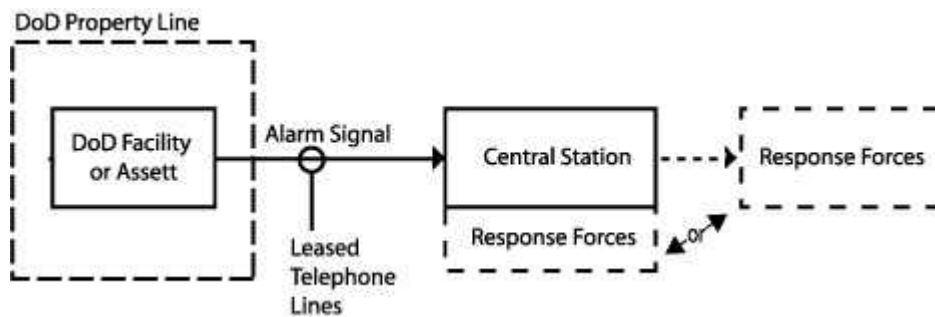
Figure 2-9. Local Alarm Monitoring.



2-5.4 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. Other connection options are dial-up modems with cellular backup and the Internet. Refer to Figure 2-10.

Figure 2-10. Central Station Monitoring.



2-5.5 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 may be used for highly valued assets not located on a DoD base or installation. Refer to Figure 2-11 for a diagram of a police station connection.

Figure 2-11. Police Connection Monitoring.



2-5.6 Summary.

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

Table 2-3 Pros and Cons of Monitoring Methods.

	Pros	Cons
Proprietary Station	Not reliant on outside sources. Can be equipped with CCTV monitoring capability for alarm assessment, video analytics, and general surveillance.	Requires 24/7 trained personnel; possibly increased staffing. Requires real estate space and fit-out hardware. Increased recurring labor cost of Dispatch Center operators.
Local Alarm	Easy to implement Cost effective Simple	No guaranteed response, relies on support forces being in audible/visual range
Central Station	Does not require any additional space or building Probably does not require any additional staffing	Requires an existing Central Station Some complexity in establishing connection May rely on non-DoD forces 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. Must consider separate archiving resource Probably does not have CCTV assessment capability. Ongoing fee may be required for monitoring Interface connection is required. Systems often operate with reduced sensitivity to minimize the number of nuisance alarms.

CHAPTER 3 ACCESS CONTROL SYSTEMS

3-1 OVERVIEW.

The primary function of an ACS is to ensure that only authorized personnel are permitted ingress to a controlled area. The ACS should 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.

3-1.1 Elements.

An ACS can have many elements, including electric locks, card readers, biometric readers, door contacts, and request-to-exit devices, all monitored and controlled by a distributed processing system and one or more workstations. ACS workstations allow security personnel to enroll authorized users in the system, set user access permissions, monitor events and alarms, and run reports on past system activity. Figure 3-1 shows an example ACS configuration, and detailed descriptions of the various elements of an ACS are provided later in this chapter.

3-1.2 Methodology.

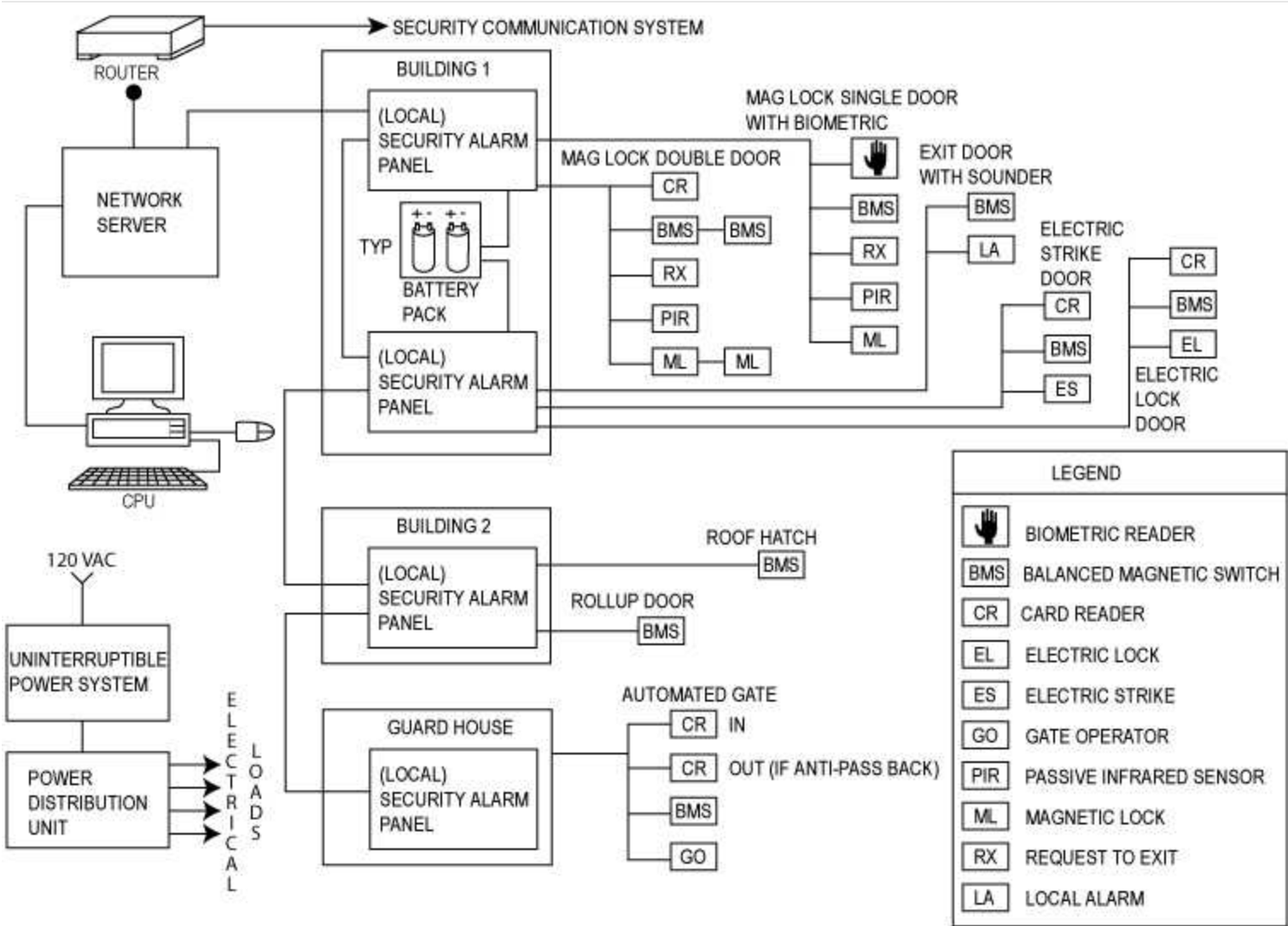
In general, an ACS compares an individual's entry authorization identifier against a verified database. If an individual's identity is verified, the ACS sends output signals to allow that authorized individual entry through controlled portals such as gates or doors. The system has the capability of logging entry attempts (authorized and unauthorized) that are archived. (Event and tracking logs are discussed in more detail in Paragraph 3-3.4 Event Tracking/Event Logs.) 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 how the ACS interfaces with the rest of the ESS is provided in Chapter 8, "ESS Subsystem Integration."

3-2 ACS ENTRY-AUTHORIZATION IDENTIFIERS.

ACS entry-authorization identifiers are grouped into three categories:

- Credential devices
- Coded devices
- Biometric devices

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



These devices operate on three basic techniques:

- Something a person has, such as a Common Access Card (CAC) \1V1/
- Something a person knows, such as a personal identification number (PIN)
- Something a person is or does, such as a biometric identifier

3-2.1 Credential Devices.

Credential devices allow a person possessing a recognized credential 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 code stored on the credential matches the code stored in the system. A credential device only authenticates the credential; it assumes a user with a recognized 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.

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

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

<p>Advantages</p> <ul style="list-style-type: none">• Cards and card readers are reliable. <p>Disadvantages</p> <ul style="list-style-type: none">• Cards can be lost or stolen.• Some types of cards can easily be duplicated. <p>Each type of card and card reader has its own advantages and disadvantages. Refer to the subsections <i>Card Readers</i> and <i>Card Types</i> in the section <i>ACS Equipment</i> in this chapter for more on the advantages and disadvantages of each.</p>
--

3-2.2 Coded Devices.

Coded devices such as keypads 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.

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.

<p>Advantages</p> <ul style="list-style-type: none">• 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. <p>Disadvantages</p> <ul style="list-style-type: none">• 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.

3-2.3 Biometric Devices.

Biometric devices rely on the comparison of a specific biological characteristic to a stored template. Fingerprint, facial patterning, hand geometry and iris scanning are the predominant biometric modalities used within DoD. 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. A one-to-many (identification) or a one-to-one (verification) 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). The verification mode generally provides faster transaction times but does require a user to present a credential or enter a code to cue a specific stored template for the one-to-one comparison. Verification is the preferred mode of operation for ACS biometric applications in DoD.

3-2.3.1 Biological Measurements.

Because of the potential differences in biological measurements made over time, the comparison of the current biological measurement with the stored template is not likely to result in a perfect match. Therefore, the algorithm allows for a small percentage of variation. While the allowed variation is small, it does raise the possibility of the two types of errors associated with ACS. The first is false reject (commonly referred to as a Type I error) where the difference between the current biological measurement and the stored template is beyond the level of acceptable variation. The second is false accept (commonly referred to as a Type II error) where an individual's biological characteristic

is sufficiently close to that of another individual that access is incorrectly granted. While biometrics can introduce both types of errors, the most likely impact will be on the overall false reject rate of an ACS. All ACS have some percentage of false positive (accept) alarm signals, and ESS system designers must 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.

3-2.3.2 Advantages and Disadvantages.

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.

<p>Advantages</p> <ul style="list-style-type: none">• They provide automated verification that the person attempting to gain access is authentic.• Biometric credentials are extremely difficult to duplicate. <p>Disadvantages</p> <ul style="list-style-type: none">• The cost is slightly higher.• Longer verification time.• Require special housings.• Some devices are not well-suited to outdoor use.
--

3-2.4 Combining Entry Authorization Identifiers.

A site's security can be significantly enhanced by combining two or more entry authorization identifiers such as a biometric characteristic with a smart card **1V1/** with a PIN code. However, combining identifiers results in increased verification time and will decrease throughput rate. Throughput time must be considered when making decisions about whether or not to use multiple identifiers. Another consideration in combining two identifiers is that a system can be required to use one identifier during lower risk times (such as during normally staffed times) and two identifiers during higher risk periods (such as nights and weekends). The same philosophy can be applied for access control enhancement during times of heightened force protection threat levels.

3-2.5 Selecting Entry Authorization Identifiers.

The type of identifier (credential, code, biometric attribute or a combination thereof) that will be used needs to be selected early in the project. This selection will drive the specifications for card readers, keypads, and biometric devices, and it will influence the layout of access control equipment at doors and other portals. The ESS designer must solicit user input concerning previously-issued credentials, such as the CAC, that may be appropriate for the ACS.

3-3 OTHER ACS FEATURES.

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

3-3.1 Anti-Passback.

Anti-passback is a functional characteristic employed within ACS. It is used to eliminate/mitigate the risk of someone giving their credential (passing it back) to another person after that credential is used to access a secure area. Anti-passback requires that a person 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. 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 software feature for Commercial-Off-The-Shelf (COTS) access control systems, but enabling this feature requires that every portal be equipped with two credential readers, one on the entry side and the other on the exit side.

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) cannot 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 cannot be used for a second entry. While affording some increased security, this process is not as rigid or secure as a “badge-out” process.

3-3.2 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.

3-3.3 Two-Man Rule.

The two-man rule is a strategy where two people must be in an area together, thus mitigating insider threats to certain critical areas. 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 card holders are logged into the area, other card 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 cards. Most ACS software will enable the assignment of a specific second person that can be established (such as clearance escort requirement).

3-3.4 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. This feature allows security personnel to query the ACS database based on specific portals, persons, or time periods of interest.

3-4 ACS EQUIPMENT.

Once the type of identifier and other implementation strategies are determined, the ESS designer must identify the type of equipment necessary to implement all required system features. Various types of ACS equipment are available, as described in the following sections.

3-4.1 Badging Equipment.

When access credentials have an associated identification badge function, ancillary badging equipment is needed. Note that besides the CAC issued to all DoD personnel, supplemental badging may be required for certain restricted access facilities. The Activity must provide justification to support the requirement for any badging equipment. Badging equipment includes:

- Camera for capturing photographs
- Software for creating badge images
- Signature capture tablet
- Biometric template capture device (where applicable)
- Badge printer capable of printing a color ID template on the front and back of the badge. 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.
- 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 client/server architecture.

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. If there is an existing system, an interface to an existing personnel database where the necessary information is stored and maintained will be required. If so, requirements for this database interface and security must be established.

3-4.2 ACS Central Computer.

The central computer is where the ACS application software and database reside and where all system activity is archived. For a small ACS, a single personal computer may be sufficient, but a large ACS may require one or more servers. A multi-server "cluster" configuration provides failover redundancy and ensures high-availability for the ACS application software and database. The central computer, together with all distributed local processors, can be thought of as the "brain" of the ACS.

3-4.3 ACS Workstation.

An ACS workstation allows personnel to view and interact with the ACS hardware and software. The central computer can function as a workstation for small systems, but a large system will likely require multiple client workstations connected to the ACS server(s) via network. The location of all ACS workstations must be identified early in the design process, recognizing that any computer with the appropriate network access and ACS software can function as a workstation.

3-4.4 ACS Local Processor.

Local processors collect inputs from card readers, keypads, biometric devices, door sensors, and request-to-exit devices, and provide output signals to electronic door locks, electric door strikes, turnstiles or gate operators. With its onboard microprocessor and memory, a local processor is able to process portal transactions even during periods when its connection to the central computer is down. This continuity is a major benefit of the distributed intelligence architecture employed by an ACS.

Local processors may employ multiple connection methods such as dial-up modem, serial (RS-232), multi-drop (RS-485), and network TCP/IP.

3-4.5 Card Readers.

The most common form of credential verification is a security card reader, and there are a number of different types. Insertion readers require that you insert the card into a slot that is just large enough to accommodate the card and then remove it. Contactless readers require that you hold the card in front of the blank face of the reader.

3-4.5.1 Insertion Readers.

Insertion readers, while functional, are generally considered less convenient for users when compared to 13.56 MHz contactless readers. This inconvenience factor, coupled with the mechanical wear associated with inserting cards favors the selection of contactless readers over insertion readers. *11*

3-4.5.2 Door Configuration.

Figure 3-5 displays a sample configuration for a single door equipped with a card reader and electric lock. Refer to the subsections on Doors and Door Locks in Chapter 9, General Requirements and Cross-Discipline Requirements for additional information on door hardware types and interface considerations.

3-4.6 Card Types.

Card readers use a number of different card types, the most common of which are described in the following subsections.

\1V1/

3-4.6.1 Smart Cards.

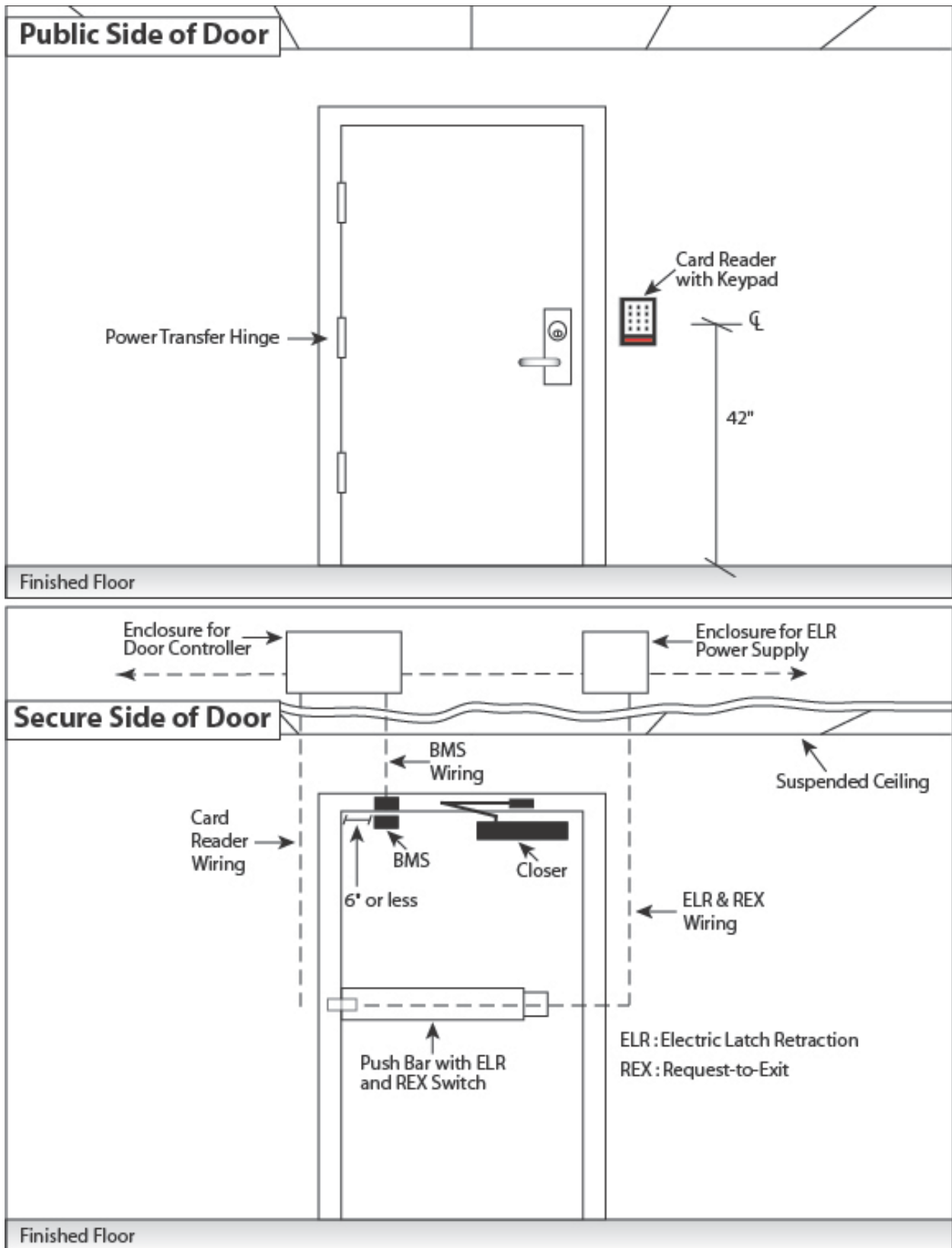
Smart cards are credential cards with a microchip embedded in them. The term “smart card” can define cards that simply carry data, but more commonly is used to describe cards with integral microprocessing and read/write data storage capability. Smart cards are available as a “Contact” type or as a “Contactless” (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 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 National Institute of Standards and Technology Federal Information Processing Standards (NIST FIPS) 201.

3-4.6.2 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 \1V1/ for legacy applications, making the card extremely versatile.

Per DoD 5200.08-R, “the CAC must be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces.” For physical access control, the contactless smart chip is the preferred feature of the CAC. However, a dual-technology smart card reader allows the contact interface to be used (via insertion) as a fallback should the contactless antenna in a card become damaged.

Figure 3-5. Sample Card Reader Door Configuration.



3-4.6.3 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 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 a credential or biometric technology. For an ACS that uses keypads as the sole entry authorization identifier, microprocessor-controlled keypads are preferred. Unlike a standard keypad, a microprocessor-controlled keypad alters the arrangement of numbers each time it is used, thereby making it more difficult for an onlooker to determine a PIN by observing which keys are pressed. Numbers are displayed on LEDs with a narrow viewing angle so that only the person directly in front of the keypad can clearly see the numbers.

3-4.8 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.

3-4.8.1 Biometric Devices.

Biometric devices are well suited for very high security areas, but may not be appropriate for portals where high throughput is a primary design objective. Designers have to evaluate the tradeoff between added security and decreased throughput.

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

3-4.8.1.1 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). This technology is mature and well understood but performance can be degraded 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 FIPS 201.

3-4.8.1.2 Facial Image.

This technology measures the geometric properties of the subject's face relative to an archived image. Specifically, the centers 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.

3-4.8.1.3 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 each hand 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.

3-4.8.1.4 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.

3-4.8.1.5 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.

3-4.8.1.6 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. Iris scanners allow scanning to occur from up to sixteen inches away. A disadvantage of iris scanning is that some people are timid about having their eye scanned. Throughput time for this technology must be considered. Typical transaction 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.

3-4.8.1.7 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 sixteen 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.

3-4.9 Request-to-Exit (REX) Devices.

Doors and other portals secured with an ACS must provide a means of authorized egress for personnel inside the controlled space. A REX device performs this function by initiating a temporary shunt of the door sensor alarm, thus allowing the ACS to distinguish between an authorized exit and an unauthorized (forced) entry. For some door configurations the REX device also releases the door locking/latching mechanism.

An ACS designer must work with the project architect to analyze each controlled door and portal to determine the appropriate REX device, taking into account security, life safety, Americans with Disabilities Act (ADA), aesthetics, ergonomics, and wiring. An overview of the four categories of REX devices is as follows:

3-4.9.1 Door Hardware.

Practically any type of door hardware can be equipped with an internal REX switch. This approach eliminates the need for an external REX device but requires that wiring be extended to the door either through an electrified hinge or exposed armored flex conduit.

3-4.9.2 Buttons.

A button labeled "PUSH TO EXIT" can be mounted on the door frame or an adjacent wall.

3-4.9.3 Motion Sensors.

A motion sensor can be mounted above the door to detect a person approaching from the secure side. This is generally considered to be the least secure REX device due to the potential for false activations.

3-4.9.4 Card Readers, Keypads, and Biometric Devices.

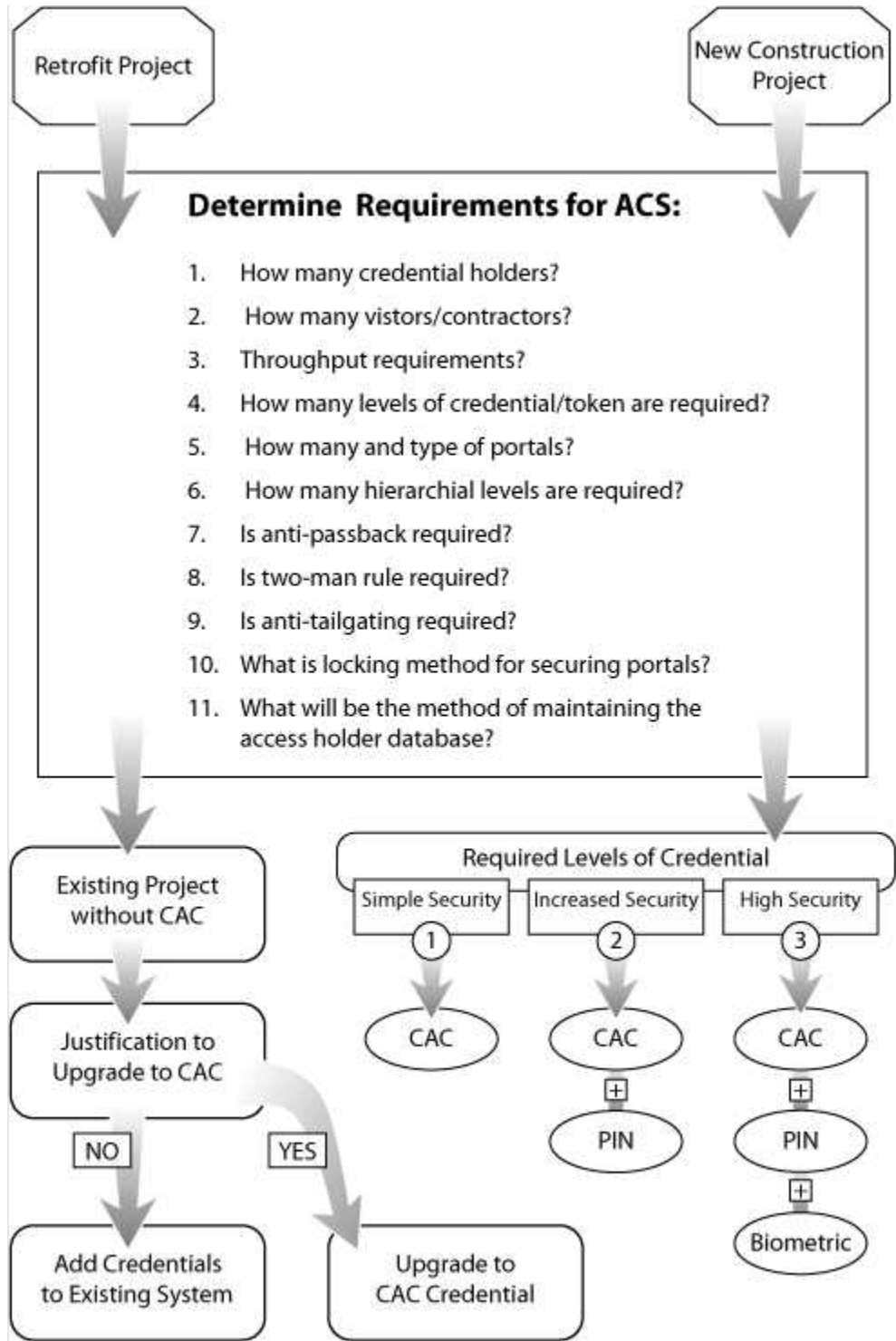
Using a card reader, keypad, or biometric device as a REX device offers the potential for “who’s in and who’s out” accountability. Refer to section 3-3 for further discussion of ACS features that require exit readers.

3-5 ACS DESIGN CONSIDERATIONS.

- a. Specify a card reader with an integrated keypad for portals where the added security of credential plus code access is required.
- b. All card readers must be UL 294 listed.
- c. Contactless card readers must conform to ISO/IEC 14443 Parts 1 through 4 and NISTIR 6887, The Government Smart Card Interoperability specification (GS-IS).
- d. For facilities requiring a higher degree of security, provide biometric capability in addition to the minimum.
- e. Per FIPS 201, fingerprint reading is the biometric technology of choice. Facial imaging is listed as a secondary biometric credential.
- f. Outside hand-geometry readers require special exterior housings. Check with manufacturer’s specifications for external applications on other biometric readers.
- g. 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.
- h. In general, the ESS designer must balance security requirements with life safety, fire-alarm interface, and normal operational convenience factors.
- i. Work with the project architect to clearly define controlled access boundaries and portals early in the design process. Specify the entry and exit function of each door on a controlled access boundary, and identify any special portal equipment such as turnstiles and security booths. Ensure that the Life Safety Plan addresses any egress restrictions associated with the ACS.
- j. Avoid using a life safety emergency exit as a high security entry portal.
- k. Limit entrances into the controlled area. SCIFs are limited to one primary entrance.
- l. Coordinate with the Architect to ensure proper doors, door frames, and door hardware are provided. For example, when an electric door strike is specified, the door frame and hardware must be checked or specified such that they are compatible with the strike in terms of wiring and latching.

- m. Consider throughput and traffic flow of normal operational traffic and emergency exiting requirements. Ensure that entry throughput at controlled portals will be adequate for the morning surge period.
- n. Additional design guidance for ACS is provided in Figure 3-6.

Figure 3-6. ACS Design Process.



CHAPTER 4 CLOSED CIRCUIT TELEVISION SYSTEMS

4-1 OVERVIEW.

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 can be integrated with ACS and IDS and may be centrally monitored at the Dispatch Center or locally monitored by security personnel at an individual facility. Uses of CCTV systems for security services include several different functions as described below.

4-1.1 Alarm Assessment.

When alerted by an alarm notification, CCTV cameras allow security personnel to visually 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.

4-1.2 Access Control.

Cameras can be used by security personnel to visually identify persons and vehicles requesting entry prior to releasing a controlled portal (door, turnstile, gate, vehicle barrier, etc.).

4-1.3 Surveillance.

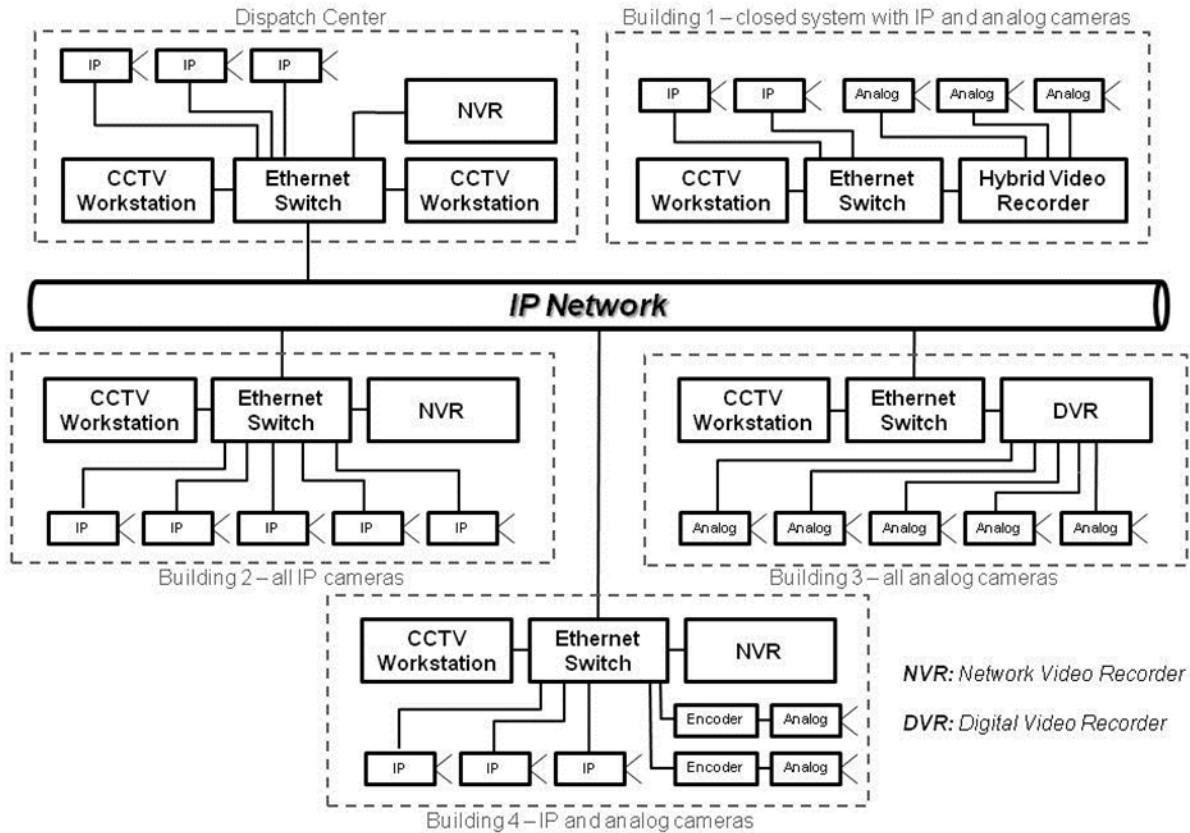
CCTV cameras can be used to give security personnel the capability to be made aware of or view visual events at multiple locations from a centralized remote viewing area. CCTV camera technology makes visual information available that would normally only be available through multiple (possibly roving) human resources. Video analytics can significantly enhance surveillance effectiveness by cuing scenes of interest and highlighting areas within scenes for priority viewing by an operator.

4-1.4 Evidentiary Archives.

Retrieval of archived images may be helpful in identification or prosecution of trespassers, vandals, or other intruders.

As shown in Figure 4-1, a large networked CCTV system may encompass several buildings and can include multiple workstations where live and recorded video can be viewed. Both analog and Internet Protocol (IP) cameras can be used to gather video images which are then stored in a digital format. Building 1 represents a closed system with no connection to an outside network, in which case all video recording, viewing and management is done within the building.

Figure 4-1. Example Block Diagram for a Networked CCTV System.



4-2 CAMERAS.

Selecting the appropriate cameras is critical to a CCTV design. The following paragraphs provide guidance regarding basic camera types and features.

4-2.1 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 than color cameras under low-light 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.

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 foot-candle (fc) (10 lux) of scene illumination, whereas a black and white camera might only require 0.1

fc (1 lux). These lighting level requirements vary with the camera model and manufacturer, so be sure to specify the appropriate illumination level for the scene of interest.

4-2.2 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:

- Sturdy, secure mounting.
- Auto-iris for lighting control.
- 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.
- To be mounted in a position to prevent glare from overhead lighting.

4-2.3 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:

- a. 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, video motion detection systems can register a false positive when plants in the field-of-view move in windy conditions.
- b. Provide heaters in cold weather applications.
- c. 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.
- d. Use caution when mounting a camera behind glass. If you mount a camera behind glass, such as in 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.

- e. 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.
- f. 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.
- g. 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.

4-2.4 Fixed Position Cameras.

After being mounted, aimed, and focused by an installer, a fixed position camera provides a field of view that cannot be changed via remote control. When used for visually assessing intrusion or access control alarms, fixed cameras are good for review of pre-alarm conditions because there is a constant view of the scene in which the alarm was triggered. Pre-alarm allows the review of video information for the time period (typically ten to fifteen seconds) immediately before the alarm occurred. Pre-alarm video is often the most useful video content for determining the actual cause of the alarm. Because of their static field of view, fixed cameras are well suited for video motion detection, but are not able to track a target of interest after it leaves the camera scene. The installation and cost of fixed cameras is lower because there is no associated motor and control wiring.

4-2.5 Pan/Tilt/Zoom (PTZ) Cameras.

A PTZ camera contains a motorized mechanism for adjusting camera aim point and lens focal length, thus allowing an operator to dynamically change the field of view via remote control. This gives the operator a much better view of the overall area compared to a fixed camera. PTZ cameras are often used for both alarm assessment and video surveillance applications; however, they are not well-suited for pre-alarm assessment because they may not be focused on the alarm area at all times. Because of the drive motor, housing, and wiring for controls, PTZ cameras are typically three to four times more expensive than fixed cameras. Table 4-1 compares other salient parameters of fixed and PTZ cameras.

A PTZ camera can be controlled by an operator or it can be programmed to perform a guard tour during which it moves sequentially through a series of user-defined preset views. When not under operator or guard tour control, a PTZ can be set to return to a

home position preset corresponding to the most important scene of interest. Preset views for alarm conditions can be programmed to override operator control, guard tour, and home position.

Table 4-1. Fixed versus PTZ Cameras.

	Applications	Cost	Pre-alarm Review	Video Motion Detection	Intruder Tracking Capability
Fixed	Alarm assessment for doors, gates and fence lines	Lower	Recommended	Recommended	None
PTZ	Surveillance for large open areas such as ports and airfields	Three times more expensive than a fixed camera	Poor application	Only for fixed, preset scenes	Good

4-2.6 Dome Cameras.

A dome camera is 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 camera's aim point. The variety of dome cameras is extensive, giving the designer a dome option for nearly any security application: fixed or PTZ, indoor or outdoor, full-size or mini-dome, analog or IP. A common application of dome cameras is in office buildings with suspended ceilings where aesthetics and ease of installation are important factors. PTZ dome cameras can move quickly from a home position to any preset, typically in less than two seconds.

4-2.7 IP and Analog Cameras.

A CCTV camera can be specified as either IP or analog, depending on the required video output format. As illustrated previously in Figure 4-1, an IP camera connects directly to an Ethernet switch from which the camera signal can be transmitted to any network node for viewing or recording. An analog camera typically connects to a digital video recorder from which live or recorded video can be transmitted to one or more CCTV workstations on the network. To ensure reliable video storage and viewing, IP cameras generally require a network with high bandwidth, high availability, and low latency.

4-3 ILLUMINATION.

4-3.1 Illuminance.

The CCTV designer must coordinate with the project's lighting engineer, landscape architect and interior designer to ensure that illuminance within scenes of interest is sufficient for cameras to render full video. Meeting this objective involves analyzing two parameters - faceplate illuminance and scene illuminance - which are illustrated in Figure 4-2 and related by the following equation:

$$C = BR \left(\frac{T}{4N^2} \right)$$

where

C = faceplate illuminance (units are foot-candles or lux)

B = scene illuminance (units are foot-candles or lux)

R = scene reflectivity factor (dimensionless number between 0 and 1)

T = lens transmittance efficiency (dimensionless number, typical value is 0.8)

N = lens f-number (ratio of lens focal length to aperture diameter)

To illustrate the use of this equation, consider the following example:

A specific outdoor fixed camera has been proposed for use at an aircraft parking area. Examining the manufacturer's data reveals that the camera requires 0.0007 foot-candle of illuminance at the faceplate to generate useable video. To achieve the desired field of view, a 5-mm lens with an f-number of 1.6 and transmittance efficiency of 0.8 is proposed. During a nighttime lighting survey it is determined that the scene of interest includes dark-colored rotary wing aircraft parked on asphalt concrete. The reflectivity factor for this scene is estimated to be 0.07. Noting that existing light fixtures are in place, light meter readings are taken at several locations within the scene and the average illuminance value is calculated to be 1.2 foot-candle. Using this average scene illuminance, faceplate illuminance is calculated as follows:

$$C = (1.2)(0.07) \left[\frac{0.8}{(4)(1.6)^2} \right] = 0.007 \text{ footcandles}$$

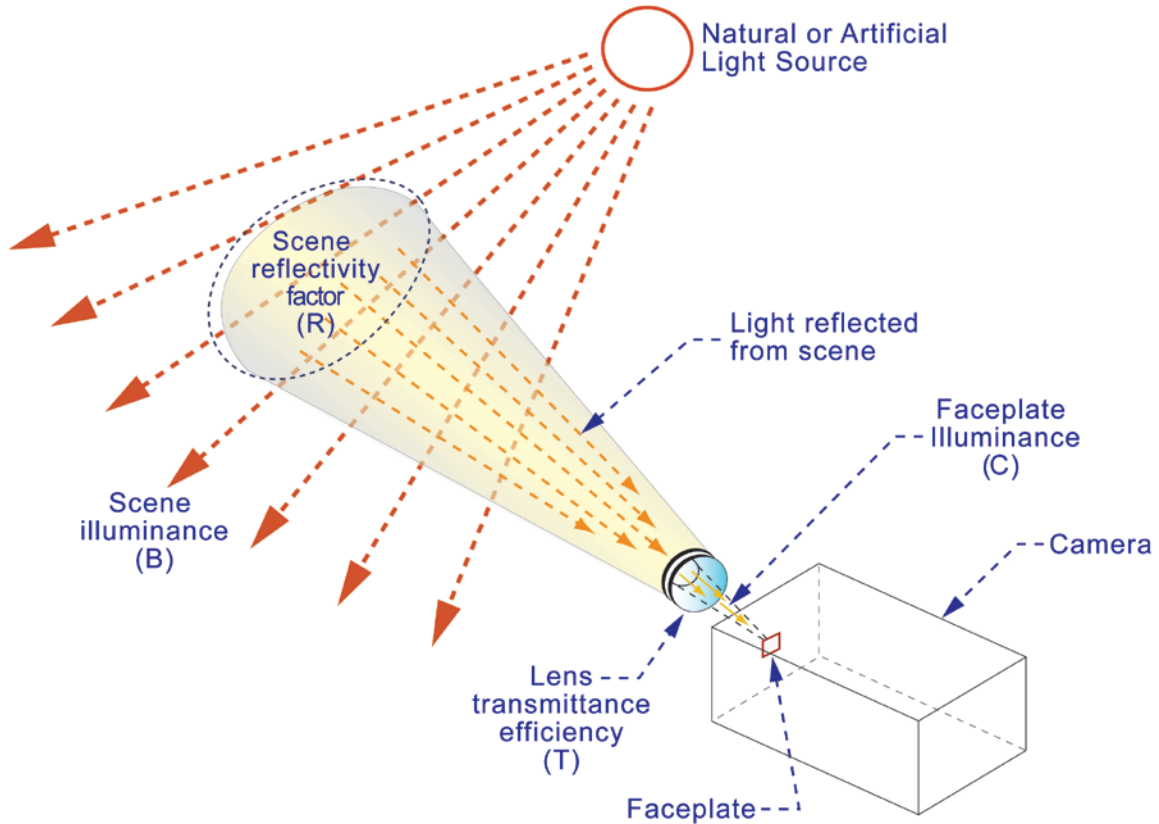
Comparing this calculated value with the manufacturer's specification (0.0007 foot-candle) indicates that existing nighttime illumination at the aircraft parking area is more than adequate to support full video capture by the proposed camera.

4-3.2 Uniformity.

Uniform illuminance within a camera scene yields the highest video quality. While not always achievable, the designer should strive for an average-to-minimum uniformity ratio of 4:1 within a scene of interest. Video quality degrades noticeably when the

uniformity ratio exceeds 8:1. For additional guidance on uniformity and other CCTV illumination parameters, refer to UFC 3-530-01.

Figure 4-2. Scene Illuminance and Faceplate Illuminance.



Reflectivity factors for a range of surface conditions are presented in Table 4-2, and these values can be used to estimate reflectivity for actual scenes of interest.

Table 4-2. Reflectivity Factors for Various Surface Conditions.

Scene Description	Reflectivity Factor
Asphalt concrete	0.07
Grass and trees	0.2
Red brick	0.35
Portland cement concrete	0.4
White matte painted surface	0.6
Glass window or wall	0.7
Snow-covered surface	0.85

4-3.3 Glare Reduction.

Glare is very detrimental to CCTV camera performance as illustrated in Figure 4-3. Glare reduction can be achieved by specifying full cut-off luminaires and insuring that luminaires are not in a camera's field of view. In general, the source of illumination is best located above the level of the camera. The CCTV designer must coordinate with the lighting designer to ensure that these glare-reduction objectives are met.

Figure 4-3. Effect of Glare on CCTV Camera Image Quality.



4-3.4 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.

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

Both of these techniques enable cameras to function more effectively in interior low-light conditions and are 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 for CCTV camera assessment.

4-4 VIEWING IN LOW-LIGHT CONDITIONS.

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.

4-4.1 Black/White Switching.

Many 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.

4-4.2 Infrared Illuminators.

The human eye cannot see infrared light. Most monochrome CCTV (black/white) cameras, however, can. Thus, invisible infrared light from either an LED or laser source can be used to illuminate a scene, which allows night surveillance without the need for additional artificial lighting. IR illumination patterns can be matched to camera field of view. A variety of patterns are available ranging from narrow- to wide-angle and short- to long-range coverage. LED IR illuminators are a good choice for short-range flood coverage and medium-range spot coverage. Approximate coverage ranges for a 26-watt LED illuminator are 65 feet (20 m) for a 120-degree flood pattern and 310 feet (95 m) for a 10-degree spot pattern. Laser IR illuminators should be considered when the desired coverage range exceeds the capabilities of LED illuminators. For example, a 60-watt laser IR illuminator can project a 10-degree pattern to a maximum effective distance of approximately 2300 feet (700 m). Infrared provides the following benefits over conventional lighting:

- Extended service life - up to 10 years.
- Lower running costs (but higher installation costs).
- Covert surveillance - no visible lighting to alert or annoy neighbors.

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, unless the color camera has an automatic black-and-white switching feature. Cameras will not render color images when used under infrared illumination. The range that the camera will see in the dark depends on sensitivity and spectral response of the camera and lens combination. 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 must not have an infrared filter. Dual mode cameras that can switch from color to monochrome operation in low light conditions must not have an infrared filter for the reason cited above.

4-4.3 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 energy 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 in comparison to visible light cameras. The disadvantage of thermal-imagers is the high cost and the inability to discern facial features and other fine details in the scene.

Typically thermal imagers are classified as medium or long wavelength as illustrated in Table 4-3. For security applications in which the object of interest is a man-size target within a few hundred meters of the camera, uncooled long-wavelength imagers are preferred because of their lower cost, both in terms of initial purchase and lifecycle maintenance. Cooled medium-wavelength imagers, though more costly, can resolve very small thermal gradients and, equipped with the appropriate lens, can capture images of man-size targets at ranges out to a few thousand meters.

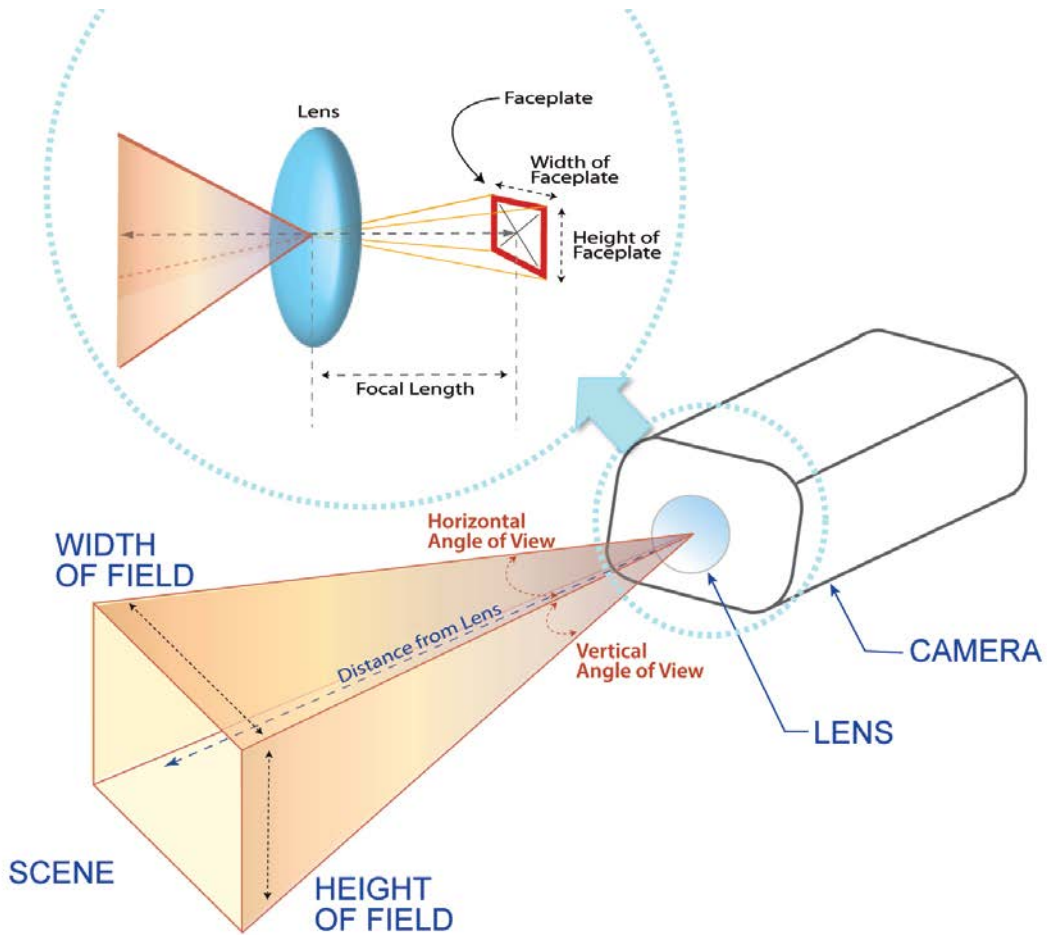
Table 4-3. Characteristics of Thermal Imagers.

Classification	Wavelength	Cooling	Cost	Recommended Service Period
Medium Wavelength	3- 5 microns	Cryogenically cooled	\$50K - \$150K	7,500 hours
Long Wavelength	7-14 microns	Uncooled	\$5K - \$50K	30,000 hours

4-5 ANGLE OF VIEW AND FIELD OF VIEW.

An important consideration when designing a CCTV system is determining the desired field of view for each camera. Field of view and angle of view are illustrated in Figure 4-4. Based on the desired field of view, the designer must specify the appropriate camera mounting location, aim point, format, and lens focal length to capture the required image.

Figure 4-4. Angle of View and Field of View.



Camera format refers to the nominal diagonal measure of the image sensor (also called the faceplate), and typical sizes are shown in Table 4-4. Given the faceplate dimensions and the lens focal length, the angle of view for any camera-lens combination can be calculated as follows:

$$\alpha = 2 \tan^{-1} \frac{l}{2f}$$

where

α = angle of view (horizontal or vertical)

l = length of image sensor (width or height, refer to Table 4-4)

f = focal length of lens

A relatively narrow angle of view would be provided by a 2/3-inch format camera equipped with 50-mm lens. In this example, the angles of view would be as follows:

$$\alpha_{horizontal} = 2 \tan^{-1} \left[\frac{8.8}{(2)(50)} \right] = 10.1^\circ$$

$$\alpha_{vertical} = 2 \tan^{-1} \left[\frac{6.6}{(2)(50)} \right] = 7.6^\circ$$

A relatively wide angle of view would be provided by a 1/3-inch format camera equipped with 5-mm lens. In this example, the angles of view would be as follows:

$$\alpha_{horizontal} = 2 \tan^{-1} \left[\frac{4.8}{(2)(5)} \right] = 51.3^\circ$$

$$\alpha_{vertical} = 2 \tan^{-1} \left[\frac{3.6}{(2)(5)} \right] = 39.6^\circ$$

The following simple ratios can be used to perform several types of field of view calculations:

$$\frac{l_{width}}{W} = \frac{l_{height}}{H} = \frac{f}{D}$$

where

l_{width} = width of image sensor

W = width of field

l_{height} = height of image sensor

H = height of field

f = focal length of lens

D = distance from lens

To show the application of these field-of-view ratios, consider this example. A 1/2-inch format camera will be mounted on a pole located 30 feet (10 m) from a pedestrian turnstile on the perimeter of an outdoor restricted area. If the desired vertical field of view is a full-height image of each person entering the restricted area, what lens focal length is needed? Assuming a 7-foot (2,134 mm) height of field at a distance of 30 feet (9,144 mm), lens focal length can be calculated as follows:

$$f = \frac{D l_{height}}{H} = \frac{(9144)(4.8)}{2134} = 20.6 \text{ mm}$$

In this example, the designer could specify a varifocal lens to allow some fine tuning of the field of view during the installation process or later adjustment to meet a new field-of-view requirement. A 10-40 mm varifocal lens set at 20.6 mm would meet the stated objective of providing a full-height image of a person at the turnstile, but the same varifocal lens could be set to 40 mm to provide better facial detail or to 10 mm to cover an adjacent vehicle gate. Supporting calculations for these focal lengths are as follows:

$$H = \frac{D l_{height}}{f} = \frac{(9144)(4.8)}{40} = 1,097 \text{ mm} = 3.6 \text{ feet (Better Facial Detail)}$$

$$W = \frac{DI_{width}}{f} = \frac{(9144)(6.4)}{10} = 5,852 \text{ mm} = 19 \text{ feet (Cover Vehicle Gate)}$$

Table 4-4. Typical Faceplate Sizes.

Nominal Diagonal Measure	Actual Width	Actual Height
1/4 inch	3.2 mm	2.4 mm
1/3 inch	4.8 mm	3.6 mm
1/2 inch	6.4 mm	4.8 mm
2/3 inch	8.8 mm	6.6 mm
1 inch	12.8 mm	9.6 mm

4-6 CAMERA RESOLUTION.

Camera resolution refers to the “graininess” of images captured and transmitted by a camera and is expressed in terms of televisions lines (TVL) for analog cameras and picture elements (pixels) for IP cameras. Table 4-5 correlates qualitative resolution descriptions to equivalent camera specifications for both analog and IP cameras. For each scene of interest, the CCTV designer must determine the camera resolution required to achieve the desired discrimination level for objects in the scene. Visual target discrimination criteria developed by John Johnson in the 1950’s, commonly referred to as the Johnson criteria and summarized in Table 4-6, can be used to analyze the impact of camera resolution on object discrimination for any given angle of view. These criteria are based on a 50% probability of accurate discrimination by a person viewing the camera image. The following example applies the Johnson criteria to illustrate the difference in object discrimination performance between a high-resolution camera and a megapixel camera.

Table 4-5. Typical Camera Resolution Specifications.

Qualitative Description	Equivalent Camera Resolution Specification	
	Analog Camera	IP Camera
Very Low Resolution - Quarter VGA	N/A	320 X 240 pixels
Low Resolution - VHS	330 TVL	N/A
High Resolution - DVD	540 TVL	720 X 480 pixels
Megapixel Resolution	N/A	1280 X 1024 pixels (and higher)
HD 1080p Resolution	N/A	1920 x 1080 pixels

Table 4-6. Object Discrimination Levels Based on Johnson Criteria.

Discrimination Level	Meaning	Pixels required across minimum dimension	Example
Detection	An object of a specified size is present.	2	An object with minimum dimension of 60 inches in the vertical orientation is present in the scene.
Recognition	The class to which the object belongs can be determined.	8	The object is a vehicle, not people or animals.
Identification	The type of object within the class can be determined.	16	The vehicle is a sedan, not a truck, SUV or van.

A 2/3-inch format camera with a 25-mm lens will be used to visually assess outdoor perimeter intrusion alarms along a restricted area. The camera will be aimed parallel to the fence line to view objects in the clear zone. The objective is for the camera to provide recognition level discrimination for a person crawling through the clear zone. This level of discrimination will allow a human crawler to be distinguished from objects of similar size such as animals and wind-blown debris. The minimum dimension for a human crawler is 12 vertical inches (0.3 m), and applying the Johnson criteria suggests that this 12-inch (0.3 m) vertical profile must be “painted” by 8 vertical pixels on the image collected by the camera. Given the properties of the camera, lens, and object to be viewed, the following equation can be used to calculate the maximum range for “recognizing” the human crawler:

$$D = \frac{hfR_{vertical}}{p_{vertical}l_{height}}$$

where

D = distance from lens to object

h = height of object

f = focal length of lens

$R_{vertical}$ = vertical resolution of the camera in pixels

$p_{vertical}$ = vertical pixels required on object

l_{height} = height of image sensor

Converting the height of the human crawler from 12 inches to 305 mm and solving this equation yields the following result for a high-resolution (720 X 480 pixels) camera:

$$D = \frac{(305)(25)(480)}{(8)(6.6)} = 69,318 \text{ mm} = 227 \text{ feet}$$

A megapixel camera (1,280 X 1,024 pixels), by comparison, provides a maximum “recognition” range of:

$$D = \frac{(305)(25)(1,024)}{(8)(6.6)} = 147,879 \text{ mm} = 485 \text{ feet}$$

In this illustration, even though the angles of view are the same for both cameras (20° horizontal & 15° vertical), the megapixel camera has two times the effective range of the high-resolution camera.

For objects having a minimum dimension equal to their width (such as a person walking), the following equation can be used in conjunction with the Johnson criteria to calculate maximum effective range:

$$D = \frac{wfR_{horizontal}}{p_{horizontal}l_{width}}$$

where

D = distance from lens to object

w = width of object

f = focal length of lens

$R_{horizontal}$ = horizontal resolution of the camera in pixels

$p_{horizontal}$ = horizontal pixels required on object

l_{width} = width of image sensor

4-7 VIDEO FRAME RATE.

Video frame rate is an important CCTV design parameter that affects video transmission, storage, and display. A frame rate of 30 frames per second (fps) is generally considered to be “full motion video” based on the National Television Standards Committee (NTSC) analog video standard. However, the transmission and recording frame rates for digital video can be set for a range of values between 1 and 30 fps, and some IP cameras and network video recorders support frame rates up to 60 fps. For most security applications, including alarm assessment and evidentiary archives, frame rates between 4 and 10 fps are fully adequate. Higher frame rates are appropriate for surveillance applications in which a smooth video stream is beneficial to the operator, especially when using a PTZ camera. Frame rates of 24 fps and higher will be perceived as “smooth” when viewed by an operator for extended periods of time. In most digital video systems, transmission and recording frame rates can be

programmed to automatically change in response to an external event such as an intrusion alarm or an internal video motion detection trigger.

4-8 DIGITAL VIDEO BANDWIDTH.

The CCTV designer must coordinate closely with the appropriate network designer or administrator to ensure that network bandwidth will support digital video transmission. Estimating bandwidth requirements using the equation below will aid in this coordination.

$$b = krz$$

where

b = bandwidth required for a single video stream

k = network overhead factor, typical value is 1.4

r = video frame rate

z = average compressed file size of a single video frame

The average file size for a single frame is dictated by the video resolution and compression, and typical values are given in Table 4-7. The following example illustrates the use of this table and the equation above.

Four IP cameras will be installed in an administrative building as part of an access control upgrade. One fixed camera will be installed at the main entry door and the other three fixed cameras will be installed at doors designated for emergency exit only. Each camera has megapixel (1280 X1024) resolution and H.264 video compression. Video from the administrative building will be transmitted via network at 5 fps to a headquarters building for recording and viewing. How much network bandwidth is required to support these four cameras?

Assuming that the main entry camera will have high scene activity, a single video frame will have an average compressed file size of 72 kB. The other three cameras will each have low scene activity and a corresponding file size of 36 kB. Using these file size values from Table 4-7, along with the specified frame rate of 5 fps, the following bandwidth estimates can be made, with the results expressed in units of Megabits per second (Mbps):

$$\text{ENTRY DOOR CAMERA: } b_{\text{entry}} = (1.4)(5)(72) = 504 \text{ kBps} = 4.03 \text{ Mbps}$$

$$\text{EXIT DOOR CAMERA: } b_{\text{exit}} = (1.4)(5)(36) = 252 \text{ kBps} = 2.02 \text{ Mbps}$$

$$\text{TOTAL FOR ALL CAMERAS: } b_{\text{total}} = b_{\text{entry}} + 3b_{\text{exit}} = 10.09 \text{ Mbps}$$

(Note: 1 Mbps = 125 kBps)

Based on this calculation, the four IP cameras will require approximately 10 Mbps of network bandwidth to transmit video from the administrative building to the headquarters building.

Table 4-7. Single-frame File Size for Various Resolution Values and Compression Schemes

Resolution (H x V pixels)	Average Compressed File Size (kB) for a Single Video Frame		
	H.264 - Low Scene Activity	H.264 - High Scene Activity	MJPEG - High Quality
320 X 240	4	8	20
720 X 480	12	24	60
1280 X 1024	36	72	180
1920 X 1080	50	100	250

4-9 DIGITAL VIDEO RECORDING.

The CCTV designer must plan for digitally recording video from all cameras, and several technology options are available. The following paragraphs provide a brief overview of four of the most common video recording methods followed by an explanation of how to estimate video storage requirements.

4-9.1 Memory Card.

Several camera models have a built-in memory card which allows video to be recorded at the edge of the CCTV system. This ensures uninterrupted recording even when the connection between the camera and the central system is lost, but storage capacity is very limited. An SD card, for example, has a capacity of 2 GB.

4-9.2 Digital Video Recorder (DVR).

A DVR digitizes analog camera inputs and stores the video on one or more internal hard drives. The number of camera inputs ranges from 4 to 32, depending on the model selected. Recording resolution up to 720 X 480 at 30 fps is available on many models. Access to live and recorded video from remote workstations is enabled by a network interface card in the DVR, but video will continue to be recorded even if network connectivity is lost. A DVR can provide several terabytes of video storage capacity.

4-9.3 Network Video Recorder (NVR).

An NVR records digital video from multiple IP cameras and video encoders to one or more internal hard drives. The capacity and sophistication varies greatly within this category of video recording technology. A low-end NVR can typically record up to 16 cameras at 30 fps, with recording resolution no greater than 720 X 480. A high-end NVR can accommodate 50 or more cameras, recording each camera at 24 fps with HD 1080p resolution. All NVRs have an internal network interface card to receive and distribute IP video streams, and high-end units have two or more Gigabit Ethernet ports. A CCTV designer must ensure that each network path connecting an IP camera with its associated recording node is adequate in terms of both availability and bandwidth. NVR

storage capacity ranges from 1 TB at the low end of the category to greater than 10 TB for high-end units.

4-9.4 Hybrid Video Recorder (HVR).

Combining the functionality of a DVR and an NVR into a single unit, an HVR can digitize and record multiple analog camera inputs while simultaneously recording multiple IP video streams. Many HVRs provide up to HD 1080p recording resolution for IP cameras, and HVR video storage capacities generally range from 2 to 10 TB.

4-9.5 Required Storage Capacity.

Once all cameras have been specified for a project, the CCTV designer should use the following equation to estimate the required storage capacity for each video storage device:

$$s = trz$$

where

s = required video storage capacity for a single camera

t = required video storage duration

r = video frame rate

z = average compressed file size of a single video frame

The following example illustrates the methodology and calculations needed to estimate required video storage capacity for a single storage device.

The CCTV system for an access control point will be upgraded. All existing components, with the exception of two analog PTZ cameras, will be removed and replaced with 5 new megapixel IP cameras, all fixed, and an NVR. Video encoders will be used to convert the analog camera signals to IP video streams which will be recorded to the NVR along with the 5 IP camera feeds. The security manager has stated that the fixed cameras will be recorded at 4 fps with a resolution of 1280 X 1024, and the PTZ cameras will be recorded at 10 fps with a resolution of 720 X 480. The security manager also stated that there is a 7-day video storage requirement for all access control point cameras. The IP cameras and the encoders for the PTZ cameras will all use MJPEG compression. How much video storage is required for the NVR?

Converting 7 days to 604,800 seconds, the storage required for a single fixed IP camera can be calculated as follows:

$$s_{\text{fixed}} = (604,800 \text{ s})(4 \text{ fps})(180 \text{ kB}) = 435,456,000 \text{ kB} \cong 415 \text{ GB}$$

The storage required for a single PTZ camera can be calculated in a similar manner:

$$s_{\text{ptz}} = (604,800 \text{ s})(10 \text{ fps})(60 \text{ kB}) = 362,880,000 \text{ kB} \cong 346 \text{ GB}$$

Taking into account the quantity of fixed and PTZ cameras, the total storage required for all cameras can be calculated as follows:

$$s_{\text{total}} = (5)(415 \text{ GB}) + (2)(346 \text{ GB}) = 2,767 \text{ GB} \cong 2.7 \text{ TB}$$

(Note: 1 TB = 1024 GB = 1,073,740,000 kB)

4-10 CCTV WORKSTATION.

To allow viewing of live and recorded video, the designer must specify at least one workstation for each CCTV system, and multiple workstations may be required for a large distributed system. Because of the computational demands associated with processing and displaying digital video streams, a “gaming” computer is a good choice for a CCTV workstation. These computers generally have high-speed processors, large amounts of RAM, fast graphics cards with high-resolution output, and network interface cards supporting Gigabit Ethernet speed. For a single-operator workstation, a graphics card feeding one or two monitors will usually be sufficient for CCTV viewing and management. If three or four monitors are needed for a workstation, two dual output graphics cards or a single quad output graphics card must be specified for the workstation. The graphics card and monitor must provide display resolution equal to or greater than the highest resolution camera in the system. Any workstation that will be used to control PTZ cameras must be equipped with a joystick. Video management software that is compatible with all cameras, encoders, and recording devices must be installed on each workstation.

4-11 VIDEO ANALYTICS.

If surveillance is an important security objective for a CCTV system, the designer must consider including video analytics as part of the system specification. Video analytics software allows the user to input a specific set of rules for each scene of interest, which, if violated, generate visual cues on the monitor, thus drawing the operator’s attention to suspicious objects or behaviors. This capability to automatically prioritize scenes and highlight suspicious areas for the operator maximizes the effectiveness of surveillance activities. Video analytics can be especially beneficial when a single operator is required to perform surveillance with a large number of cameras. Video analytics algorithms can be embedded in IP cameras, encoders, and recording devices or they can run on dedicated file servers. Common rule violations programmed to alert the operator include crossing a virtual tripwire, loitering in a prohibited area, moving in the wrong direction, leaving an unattended object, and removing an object.

4-12 CCTV DESIGN PROCESS SUMMARY.

4-12.1 Define Security Objectives for the CCTV System.

Begin by evaluating specific project requirements in light of the four most common CCTV functions: 1) alarm assessment, 2) access control, 3) surveillance, and 4) evidentiary archives. Concisely state objectives with enough detail to facilitate camera selection and layout. Example objectives are as follows:

- Visually assess perimeter intrusion alarms for seven bistatic microwave sensor zones around the satellite communications facility.
- Visually identify the driver and vehicle prior to opening the gate at the test area.
- Perform surveillance of four exhibit areas in the museum and maintain a 30-day video archive for evidentiary purposes.

4-12.2 Develop a Camera Layout to Meet the Security Objectives.

Indicate camera locations on site plans and building floor plans, identifying each camera as fixed or PTZ. Specify the mounting configuration (wall, ceiling, pole, roof, etc.) for each camera, and select the appropriate camera and lens for the intended field of view.

4-12.3 Verify That Illumination Is Sufficient For Each Scene Of Interest.

Ensure that camera specifications for faceplate illumination are met and that uniformity ratios are within acceptable limits. Specify lighting upgrades as needed.

4-12.4 Specify Workstation Locations.

Indicate workstation locations on building floor plans, and describe the basic configuration of each workstation including quantity and size of monitors. Identify any special furniture or console requirements.

4-12.5 Specify Recording Locations and Capacity.

Indicate recording locations on building floor plans, and describe the type and quantity of recording devices required at each location. Calculate the required video storage capacity for each recording device.

4-12.6 Define Network Architecture.

Develop a block diagram to illustrate connectivity for all cameras, recorders, workstations, and networking devices. Specify cables required for equipment interconnection, and calculate bandwidth requirements for all network connections.

4-12.7 Define Power Requirements.

Determine the power requirements for each component. Specify all power circuits and the location of all power supplies.

4-12.8 Describe Software and Integration Requirements.

Specify features and functions required for camera control, video management, and analytics. State alarm assessment requirements for integration with intrusion detection and access control software.

CHAPTER 5 INTRUSION DETECTION SYSTEM

5-1 OVERVIEW.

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 sensors, local processors, arm/disarm devices, workstations, and the central system along with the supporting data transmission infrastructure. These elements are shown in Figure 5-1. An IDS requires integration with a process and mechanisms for assessing and responding to intrusion alarms.

5-2 SYSTEM CONFIGURATION.

The designer must determine the appropriate IDS configuration early in the planning stage of a project. The four most important configuration issues that must be resolved are policy compliance, alarm monitoring location(s), zone definition, and IDS/ACS integration. These four issues are discussed in the following paragraphs.

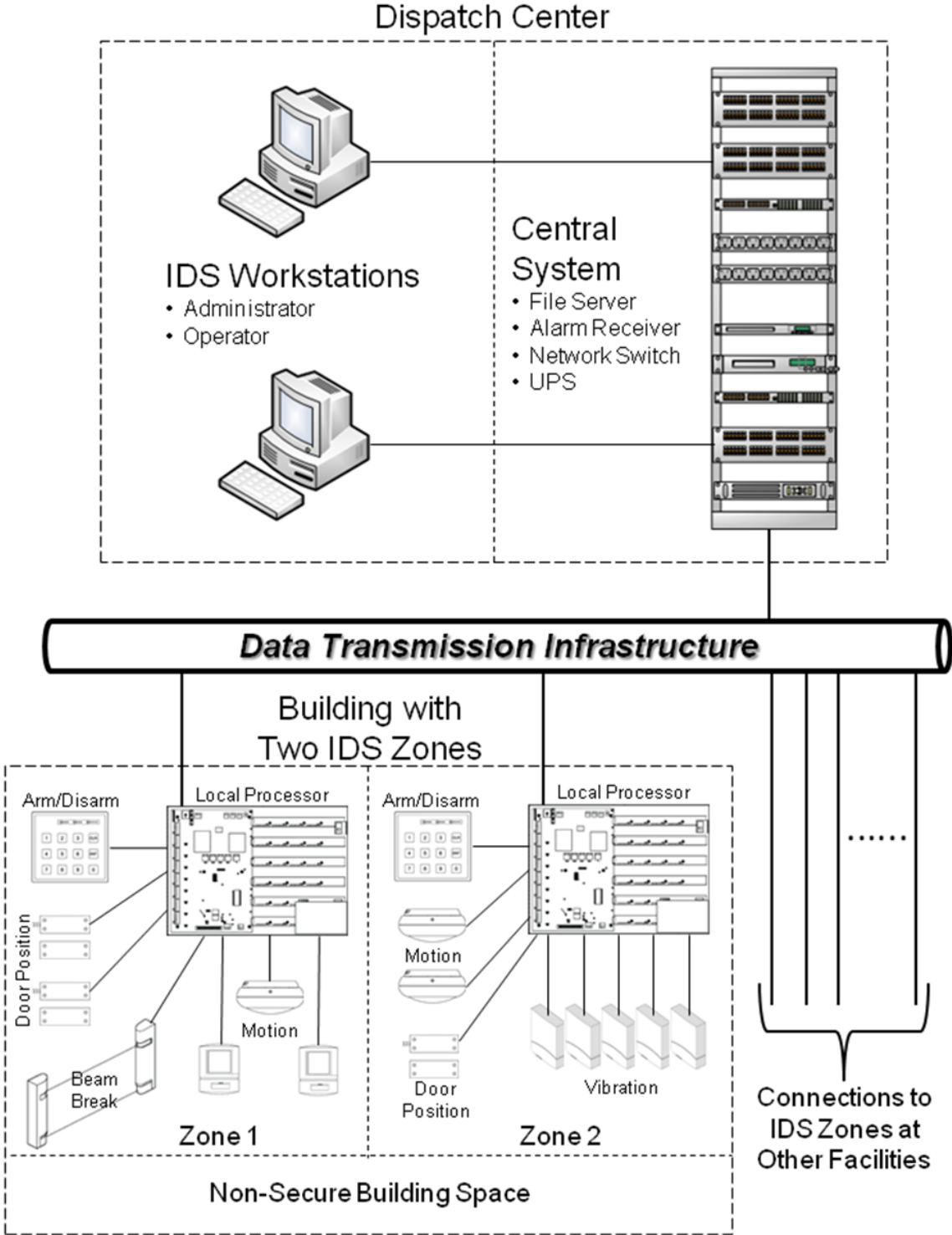
5-2.1 Policy Compliance.

Determining which assets require IDS coverage is an essential first step in the IDS design process. The designer must work closely with the facility owner/user to understand what assets are present and then determine whether or not IDS is required based on applicable security policy. The goal of this activity is to focus IDS coverage where it is required at a facility (arms room, SCIF, etc.) while avoiding frivolous investment to cover low-security areas (office suite, conference room, etc.) This activity is also beneficial in defining IDS zones as described in greater detail later in this section. Notional interior IDS configurations for a variety of assets are provided in Appendix C along with policy references for each. Examples of assets that generally require exterior perimeter IDS are special weapons (nuclear, chemical) storage facilities, high-value aircraft parking areas, and ballistic missile defense sites.

5-2.2 Alarm Monitoring Location(s).

Since most IDS requirements are focused on protecting unattended high-value assets, the designer must identify the best method for continuous alarm monitoring during periods when the secure area is not occupied. For IDS zones located in a facility that has a continuously-manned security desk, local monitoring may be the best option. Most buildings on military installations, however, do not have around-the-clock security staffing. This is especially true of smaller buildings that may have only one or two IDS zones such as an arms room or SECRET open storage area. The best option for these facilities is connecting the IDS zone(s) to a base-wide IDS with continuous alarm monitoring at the Dispatch Center. This configuration is illustrated in Figure 5-1. For some projects, it may be appropriate to provide the capability to monitor IDS alarms locally (at the security desk during duty hours, for example) and also at the Dispatch Center (primarily after duty hours).

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



5-2.3 Zone Definition.

The designer must define zones for both interior and exterior IDS. In general terms, an interior IDS zone is a room or space within a building that can be armed and disarmed independently from all other zones. The simplest interior zone is a single room with a specialized function protected by a few sensors connected to a local processor. A good example of a simple interior zone is an arms room. A large zone may encompass several adjacent rooms (to include an entire floor, wing or office suite in some buildings) or a large open area, and it may have twenty or more sensors connected to the local processor. Regardless of the size or complexity of a given interior zone, the designer should specify that each sensor annunciate as a discrete, identifiable alarm point in the IDS. Examples of interior IDS zones are provided in Appendix C. An exterior IDS zone is a continuous section of perimeter for which alarms are annunciated independently from all other alarm zones.

Like its interior counterpart, an exterior IDS zone can also be independently armed and disarmed. The designer must determine the appropriate perimeter zone layout based on the shape of the perimeter, length of each side or fence segment, location of access roads and gates, and the range capability of the candidate sensor technology. As a general rule, shorter zones enhance alarm assessment and response, but longer zones are more economical. Best practice dictates that a standard zone length of approximately 330 feet (100 m) achieves a good balance between system cost and system effectiveness and is well within the range capabilities of most sensor technologies. Another advantage of a 330 feet (100 m) zone is that alarms can be visually assessed anywhere in the zone with a single fixed camera (assuming that the appropriate lens focal length and faceplate resolution are specified). An example of an exterior IDS zone layout is shown in Figure 5-2.

5-2.4 IDS/ACS Integration.

For each ESS project, the designer must determine whether IDS and ACS functions would be best provided through a single unified IDS/ACS or through two separate systems. Even if it is appropriate to field separate systems as shown in Figure 5-3, some degree of IDS/ACS integration is often desirable. In general, any output from one system can be incorporated as an input to another system through a simple relay-to-relay integration. As an example, door held open violations from an ACS can be annunciated as alarms in a separate IDS by wiring ACS outputs to IDS inputs at the local processor level. Additional information on IDS/ACS integration is provided in Chapter 8.

Figure 5-2. Example Exterior IDS Zone Layout.

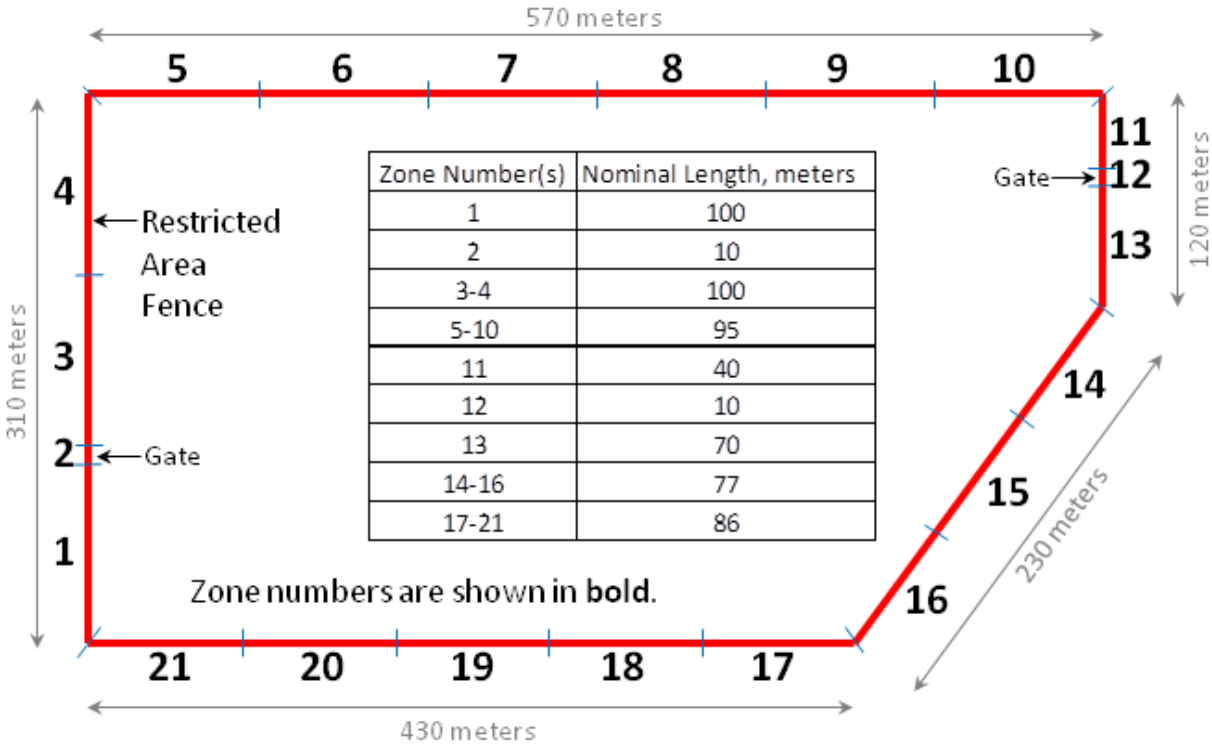
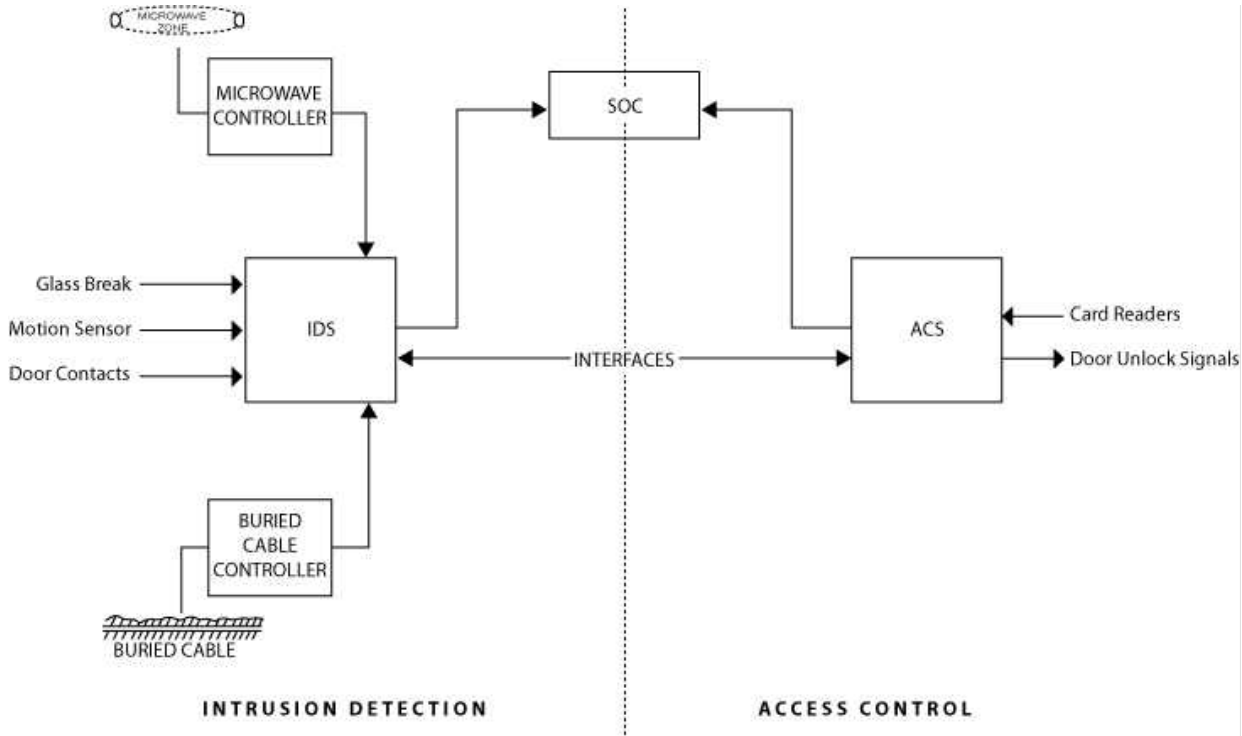


Figure 5-3. Separate ACS and IDS.



5-3 INTERIOR SENSORS.

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 O-2000.12-H. Table 5-1 provides application notes for interior IDS sensors.

5-3.1 Interior Point Sensors.

5-3.1.1 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 has 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 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 5-4, 5-5, and 5-6 show some typical applications of BMS.

Figure 5-4. Sample Door Configuration.

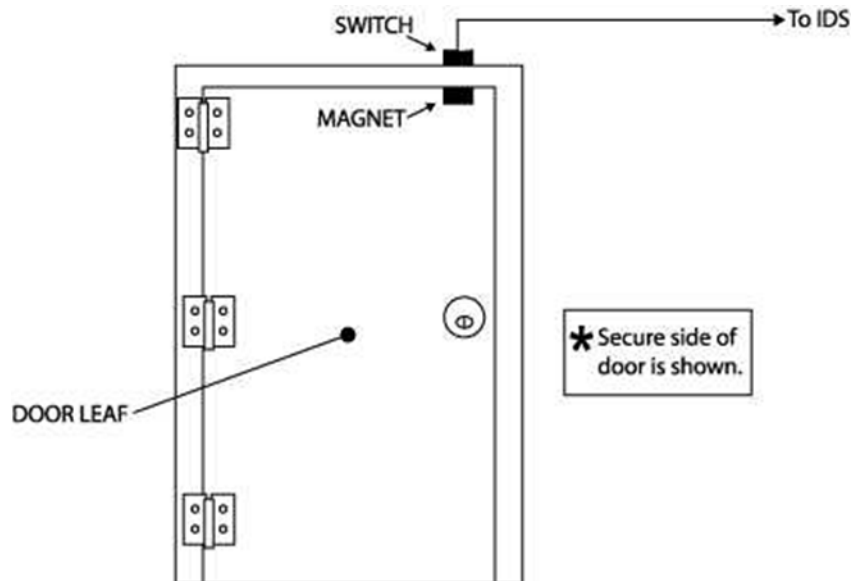


Figure 5-5. Sample Window Configuration.

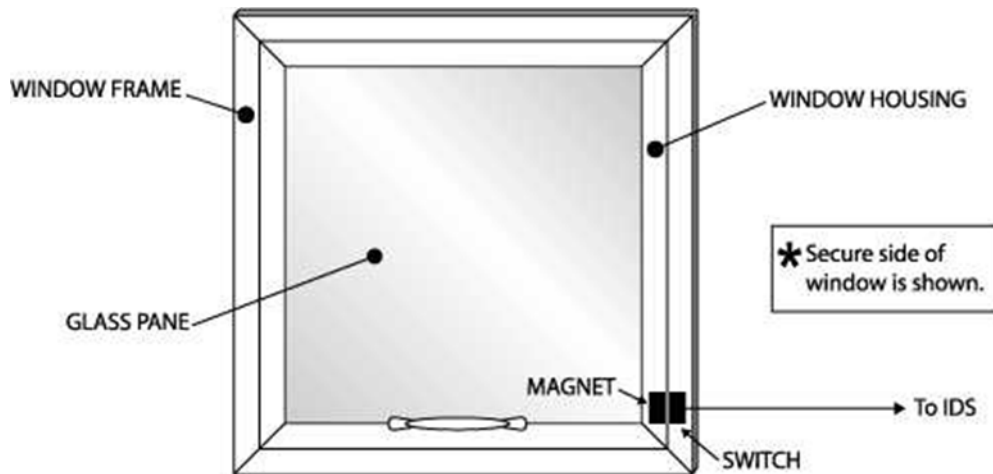
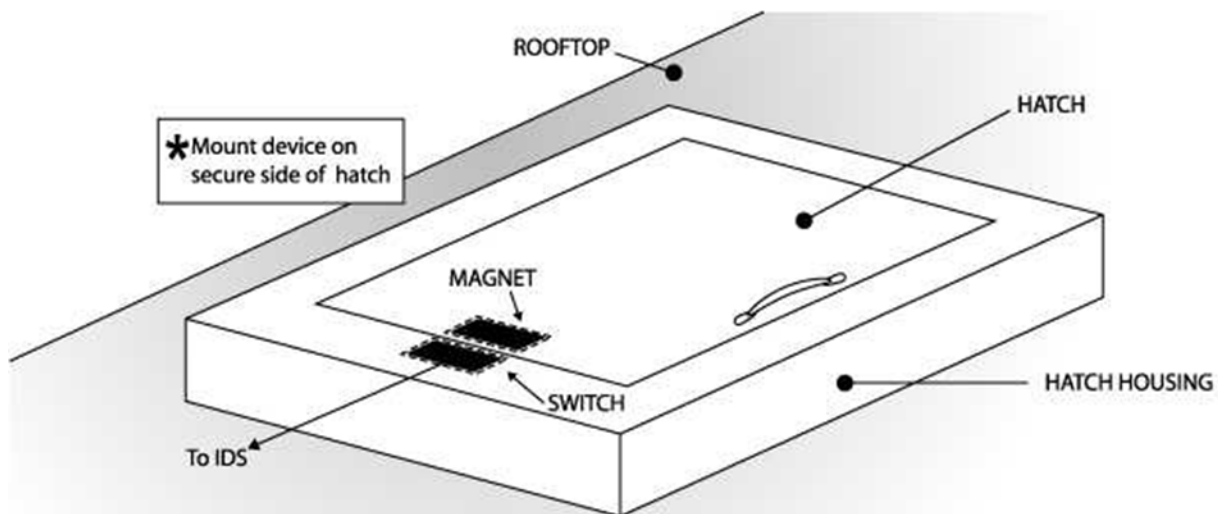


Figure 5-6. Sample Roof Hatch Configuration.



5-3.1.2 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. Glass break sensors can be used to cover multiple windows.

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 must 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.

5-3.1.2.1 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.

5-3.1.3 Glass Break Sensor Guidance.

- a. Do not use window mounted glass break sensors.
- b. Glass break sensors should only be used in protected areas with windows on the ground floor or that are easily accessible.
- c. Use volumetric sensors in conjunction with glass break sensors in protected areas.
- d. 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.
- e. Check glass break sensor specifications to ensure they are rated for the type of glass used, typically laminated glass.

5-3.2 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).

5-3.3 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.

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

5-3.4 Passive Infrared (PIR) Sensors.

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.

5-3.4.1 PIR Coverage.

Different lenses 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 narrower or wider sensor coverage area.

5-3.4.2 PIR Sensor Guidance.

- a. Use caution when specifying this sensor for areas that can be exposed to sudden changes in background environmental temperature.
- b. Best use is in interior climate-controlled spaces.
- c. 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).
- d. PIRs can also be defeated by a trained, slow-moving intruder. (Very hard to achieve.)
- e. PIRs are much more sensitive to travel crossing its sensing area as opposed to travel toward the sensor.

5-3.5 Ultrasonic Sensors.

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.

5-3.6 Dual-Technology Sensors.

Dual-technology sensors use both microwave and PIR sensor circuitry within a single 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.

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

5-4 EXTERIOR SENSORS.

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.

5-4.1 Open Terrain.

Open terrain sensors include infrared, microwave systems, combination (dual technology), and vibration sensors. In general, open terrain sensors work best on flat, cleared areas. Heavily or irregular contoured areas are not conducive to open terrain sensing systems.

5-4.1.1 Infrared Sensors.

5-4.1.1.1 Passive.

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

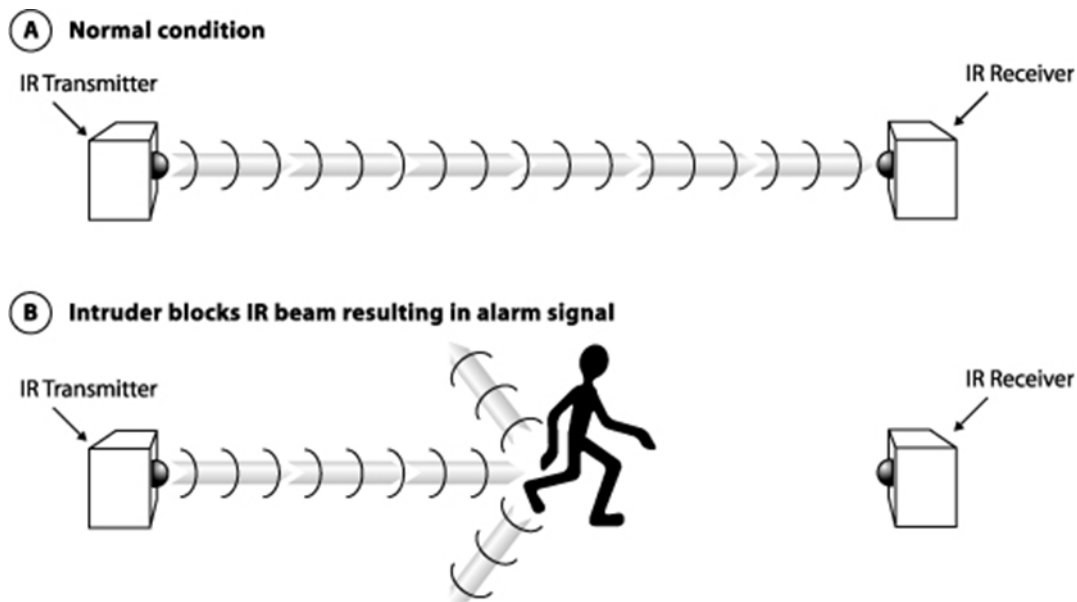
5-4.1.1.2 Active.

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 5-7 for a conceptual diagram of how an active infrared IDS works.

5-4.1.1.3 Infrared Sensors Guidance.

- a. Check that the terrain is suitable for clear signal transmission.
- b. Infrared arrays do not work well in areas with heavy snowfall because drifts or snow mounds cover sensors and or block transmission and reception paths.
- c. Shield receiver from direct sunlight.

Figure 5-7. Active Infrared IDS.



5-4.1.2 Microwave Sensors.

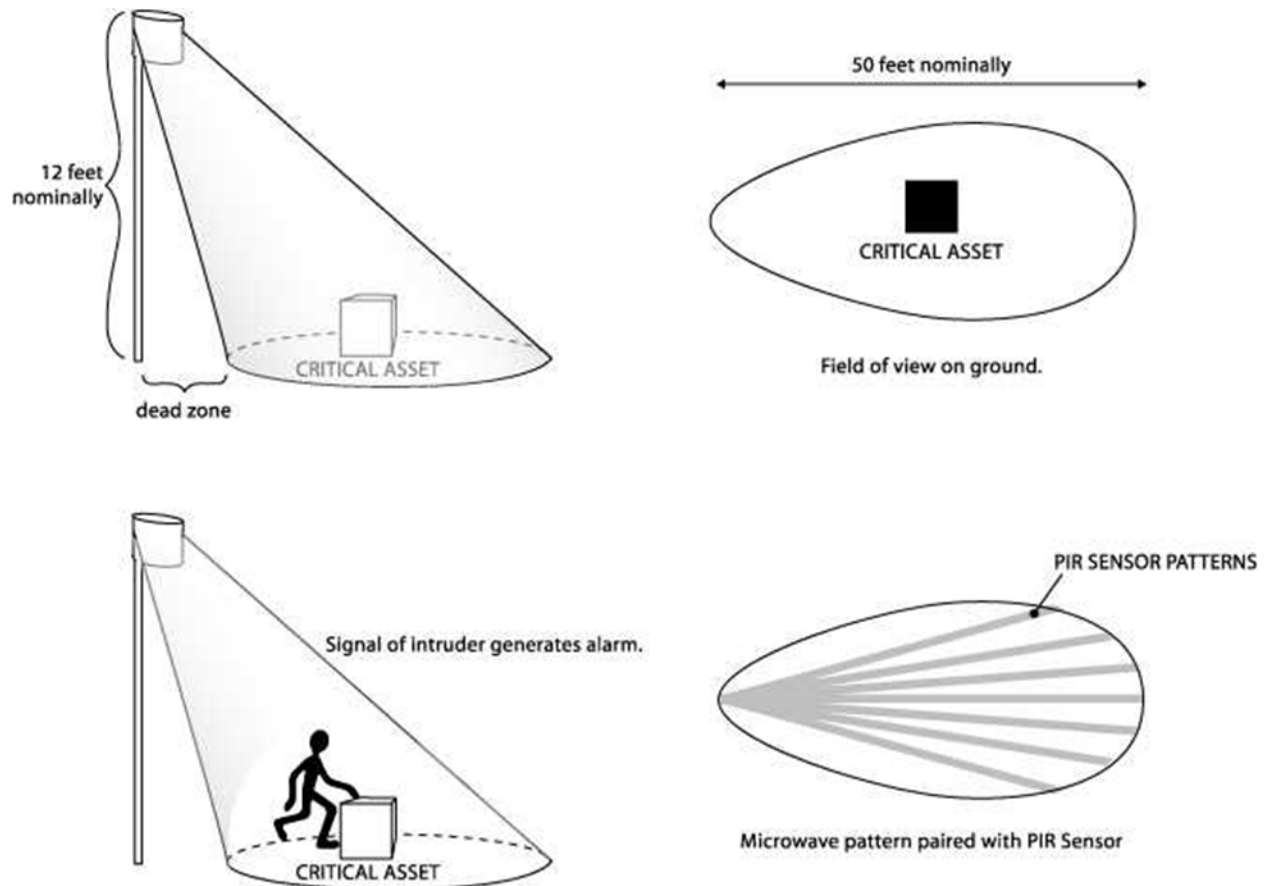
Microwave sensors come in two configurations: bistatic and monostatic. With both bistatic and monostatic sensors, the sensors operate by radiating a controlled pattern of microwave energy into the protected area. The transmitted microwave signal is

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.

5-4.1.2.1 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 5-8 for illustrations of a monostatic microwave sensor and associated footprints.

Figure 5-8. Monostatic Microwave Sensor and Associated Footprints.



5-4.1.2.2 Bistatic.

Bistatic microwave sensors are more commonly used than monostatic sensors for wide-area surveillance. Bistatic microwave sensors use a transmitter and receiver pair. Bistatic sensors work over longer distances than mono-static sensors. Typical distances for transmitter-receiver pairs are 10 - 600 feet (3 - 182 m) for X-band frequencies and

100 - 1500 feet (30 – 457 m) for K-band frequencies. The bistatic 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 K-band 24 GHz.) Refer to Figure 5-9 and Figure 5-10 for illustrations of bistatic microwave sensor operation.

Figure 5-9. Bistatic Microwave Sensor Operation.

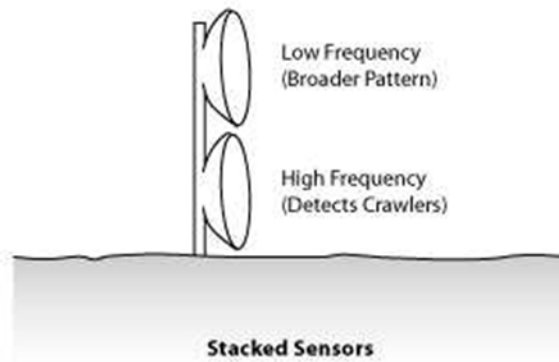
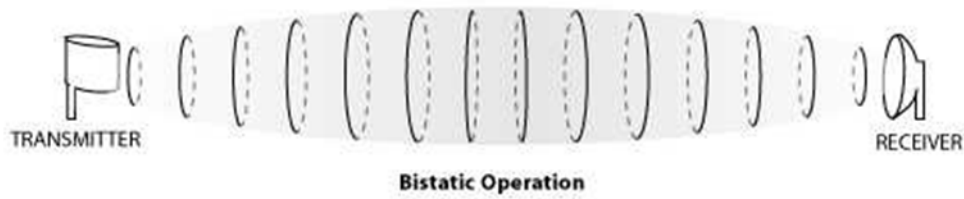
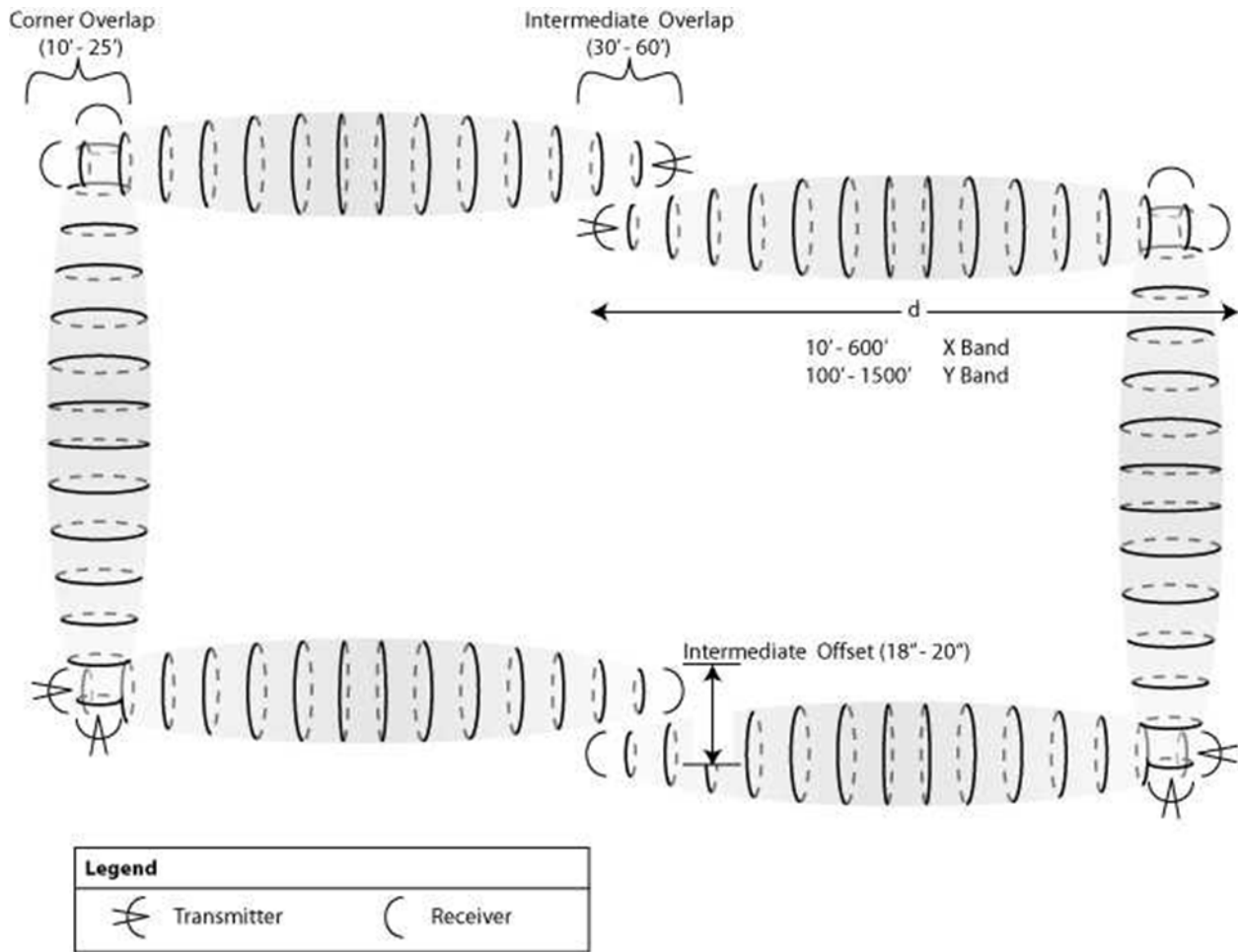


Figure 5-10. Typical Bistatic Microwave Layout and Guidance.



5-4.1.2.3 Microwave Design Guidance and Recommendations.

- a. The detection zone should be free of bushes and obstructions.
- b. The detection zone should be graded to within three inches to detect crawling intruders.
- c. 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 10 feet (3 m) by 10 feet (3 m), a 20 foot (6 m) wide gravel bed works well.
- d. Avoid water puddles. The wave action of wind on water can cause nuisance alarms.
- e. 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.

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

5-4.1.3 Dual-Technology.

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 5-6 “AND/OR” CONFIGURATION OPTIONS.

5-4.1.4 Vibration Sensors.

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.

5-4.2 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 must 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.

5-4.2.1 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.

5-4.2.2 Taut Wire Systems.

Taut-wire fence-sensing systems use a series of parallel wires under tension with 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.

5-4.2.3 Coaxial Strain-Sensitive Cable Systems.

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.

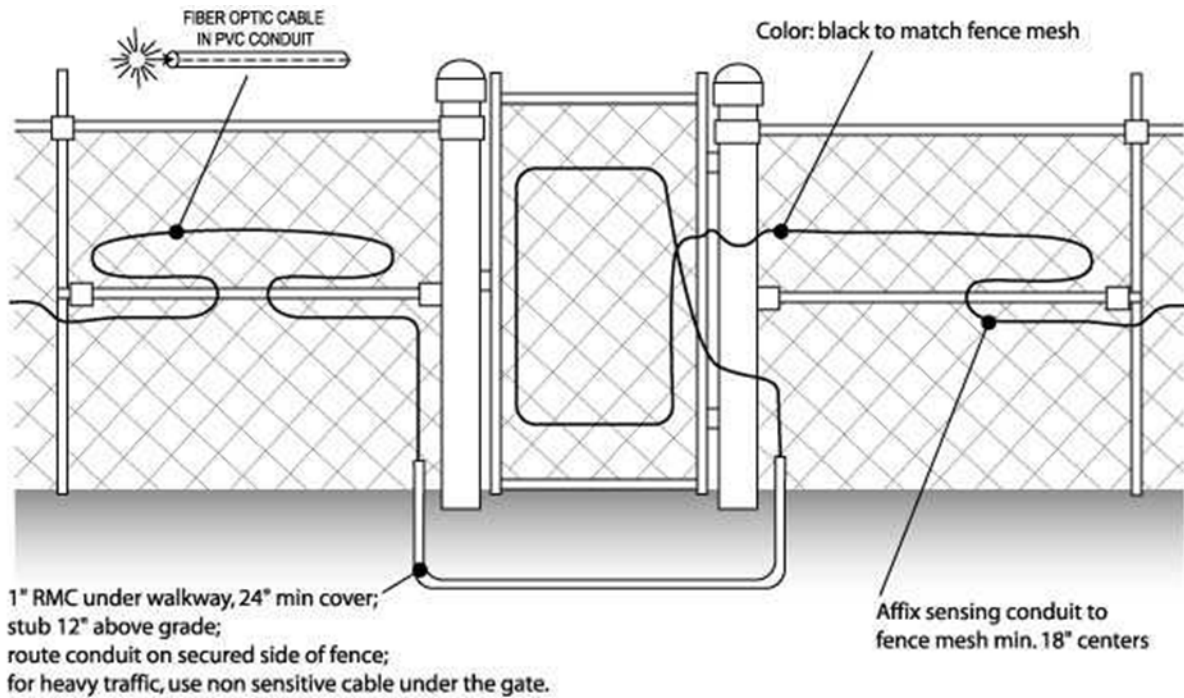
5-4.2.4 TDR Systems.

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 or 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.

5-4.2.5 Fiber-Optic Strain-Sensitive Cable Systems.

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.

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



5-4.2.6 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.

5-4.3 Other Exterior Sensors.

5-4.3.1 Buried Cable.

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 affect the sensor readings.

5-4.3.2 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 (1.8 m) in diameter around the cable. Paired cable systems use two cables routed in parallel approximately five feet (1.5 m) apart. One cable transmits and the other receives a signal to create the sensing field.

5-4.3.3 Fiber Optic.

Fiber optic lines can be used to monitor pipelines or manholes.

5-4.3.4 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.

5-4.4 Double Fence Concept.

When fence detection sensors are used, the best application is to use the double-fence concept. The typical configuration is outer clear zone, outer fence, isolation zone, inner fence, and inner clear zone, see Figure 5-12. Outer fence line defines the protected or restricted area boundary and is intended to keep animals, people, vehicles, and windblown debris out of the isolation zone to reduce nuisance alarms. No sensors should be placed on the outer fence of a double fence line system. Refer to MIL-HDBK-1013/10 (scheduled to be replaced by UFC 4-022-03, Security Engineering: Fences and Gates) for fence requirements.

Figure 5-12. Double Fence Example.



5-4.5 False Alarm Causes for Exterior Sensors.

Table 5-2 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.

Table 5-2. False Alarm Causes—Exterior IDS Sensors.

Sensor Type	False Alarm Cause	Notes
Active Infrared	Animals Wind-blown debris	Fencing mitigates animal false alarms
Passive Infrared (PIR)	Reflected light 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 Roadways—vehicles Runways—airplanes Rock quarries—explosions Seismic event	Only works well in low background vibration areas
Coaxial Strain-Sensitive	Wind flexing fence EMI	Temperamental
Fiber-Optic	Improper noise level adjustment 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 Movement of nearby vehicles or medium to large animals Congregation of small animals.	Very susceptible to EMI from large electrical equipment or substations and should not be used near these installations

5-5 VIDEO ANALYTICS FOR IDS.

Although video analytics can be very effective as a surveillance tool (see Chapter 4, paragraph VIDEO ANALYTICS), it should not be considered a primary IDS technology on par with the proven interior and exterior sensors described previously in this chapter. For most common IDS applications, traditional IDS sensors are generally superior to video analytics in terms of probability of detection, nuisance alarm rate, integration with alarm monitoring systems, and cost. The designer may consider specifying video analytics as an IDS sensor for projects where unusual site conditions bring into question the viability of all other sensor technology options.

5-6 “AND/OR” CONFIGURATION OPTIONS.

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 must be disabled. Table 5-3 displays the advantages and disadvantages of each configuration.

Table 5-3. 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

5-7 IDS DESIGN GUIDANCE.

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.

5-7.1 Critical Asset Case Study.

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 5-4.

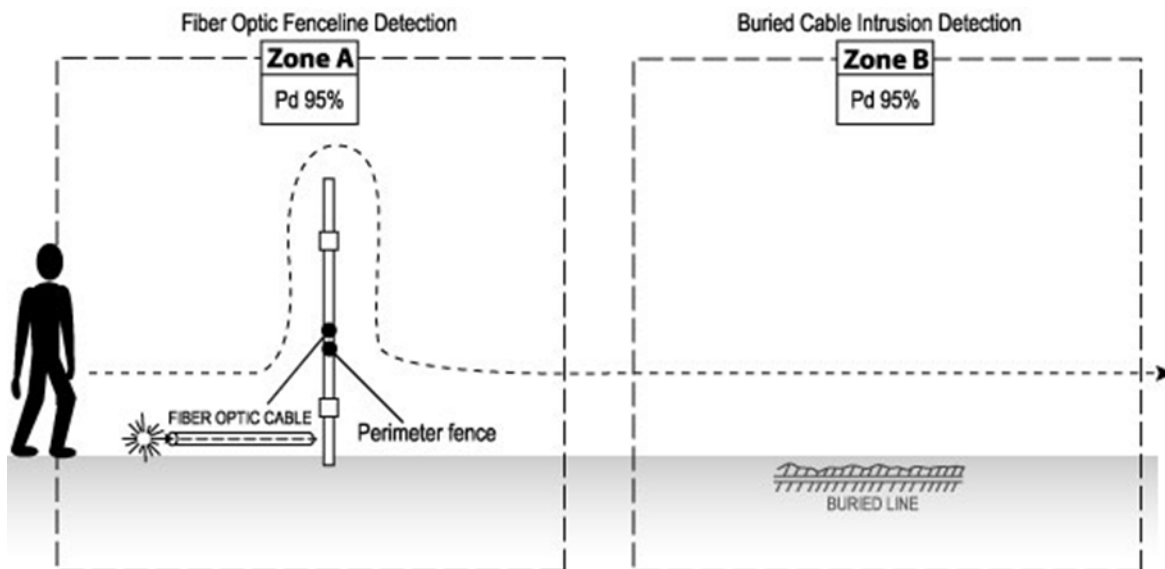
Table 5-4. Sample Probability of Detection Factors.

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

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:

- 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.
- 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.



5-7.1.2 Probability of Detection (Pd) Calculation.

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.

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:

$$\begin{aligned} &= (1-Pd) A * (1-Pd) B \\ &= 5\% * 5\% \\ &= 0.25\% \\ &= 0.0025. \end{aligned}$$

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%.

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 fence line 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.

5-7.2 Additional IDS Design Guidance.

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

Table 5-5. IDS Design Guidance.

Issue	Recommendations
Door Status Monitoring	<p>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.</p> <p>Doors for emergency egress should include an audible device (door screamer) on the secured side.</p> <p>All door monitoring should be via balance magnetic switches. The status switch contacts must be closed when the door is closed.</p>
Redundant Path for Alarms	<p>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.</p>

Table 5-6. 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.
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.
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.
<i>Note: Table is not all inclusive of all exterior sensor options. Refer to text above for more detail.</i>		

5-8 SUMMARY.

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 percent. 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.

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.

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 high-traffic conditions. This can affect network cost, reliability, and transmission speed. Of the three ESS subsystems, CCTV generally requires the most bandwidth and IDS requires the least. ACS bandwidth requirements are generally low, but bandwidth usage will spike during database synchronization cycles. For the DTM, design a system capable of handling the total bandwidth (plus contingency) for each link required in the system. Table 6-1 presents bandwidth usage values for some common ESS components.

6-3 SECURE COMMUNICATIONS.

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 conduit for all conductors, as well as electronic protection, such as encrypting communication transmissions and supervising alarm circuits. Refer to Chapter 9 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 TOPOLOGY.

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

Table 6-1. Bandwidth Usage Values.

Component	Bandwidth Usage Range (kilobits per second)		
	Low	High	High bandwidth usage results from:
IDS Local Processor	1	3	high alarm rate, encryption
ACS Local Processor	5	50	high-volume portal traffic, large database synchronizations
IP Camera	100	70,000	high frame rate and resolution, low compression ratio
ESS Workstation	100	100,000	large number of simultaneous video streams

6-4.1 General Network Topologies.

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

6-4.1.1 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 topology is that if one of the links is disabled or severed then communication is lost to that node. The unconnected node may still operate through distributed intelligence, but will be unable to receive updates from and transmit alarms to 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 was 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 topology for both an inter-site architecture and an intra-site architecture.

6-4.1.2 Ring.

The ring topology communicates through a loop. This topology is slightly more robust than a star topology in that if a link fails, communications can still be maintained through the “backside” direction on the loop. Communications may be slower in this backup mode of operation but would be sustainable. Figure 6-2 shows a ring topology for both the inter-site and intra-site scenario.

6-4.1.3 Fully Meshed.

The most robust topology is a fully meshed topology depicted in Figure 6-3. This topology has backup means of communication, such that if any one link is disabled or

severed, data has an alternate path to communicate directly between nodes. This is the preferred ESS network topology.

Figure 6-1 Star Topologies.

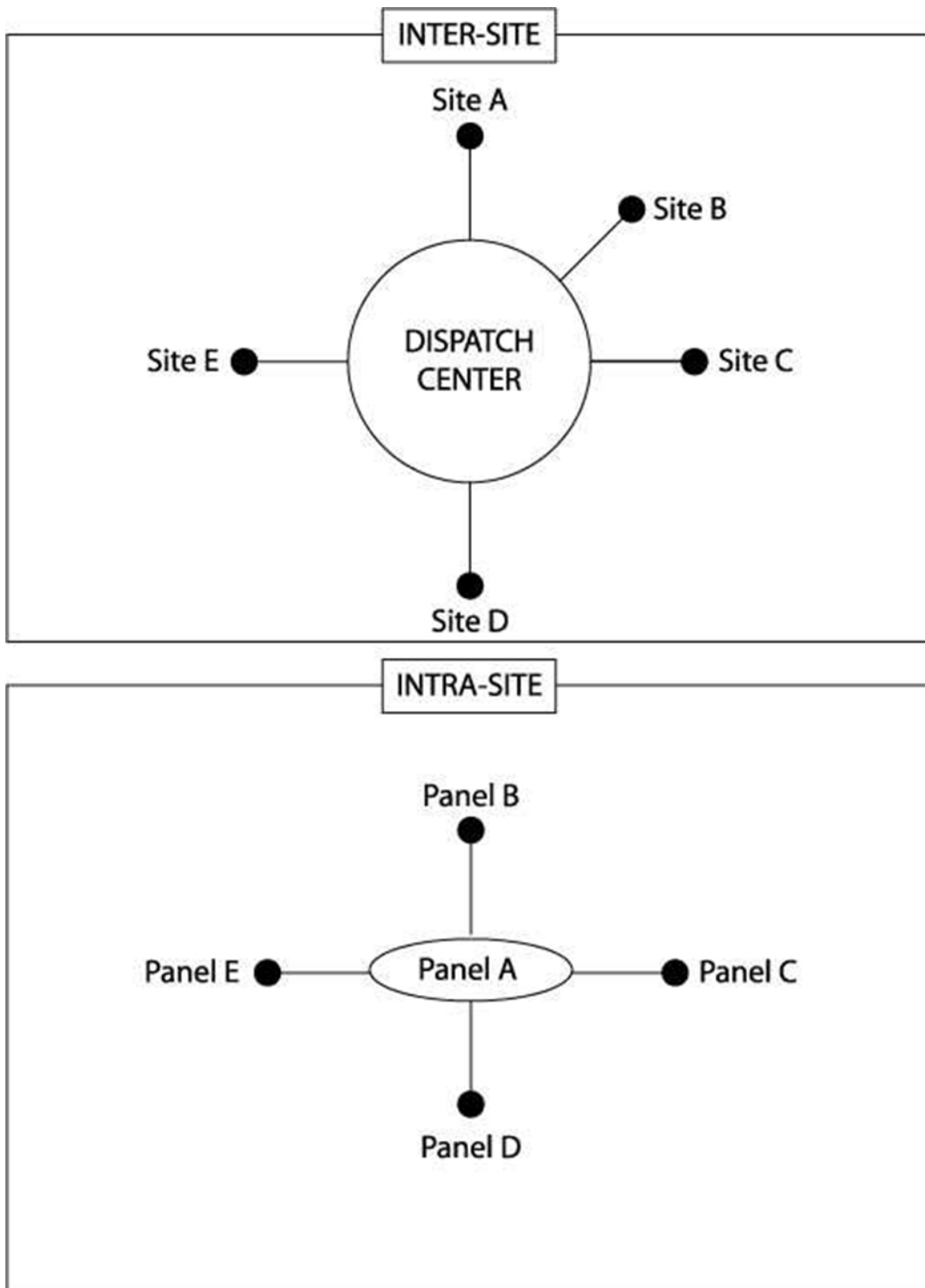


Figure 6-2. Ring Topologies.

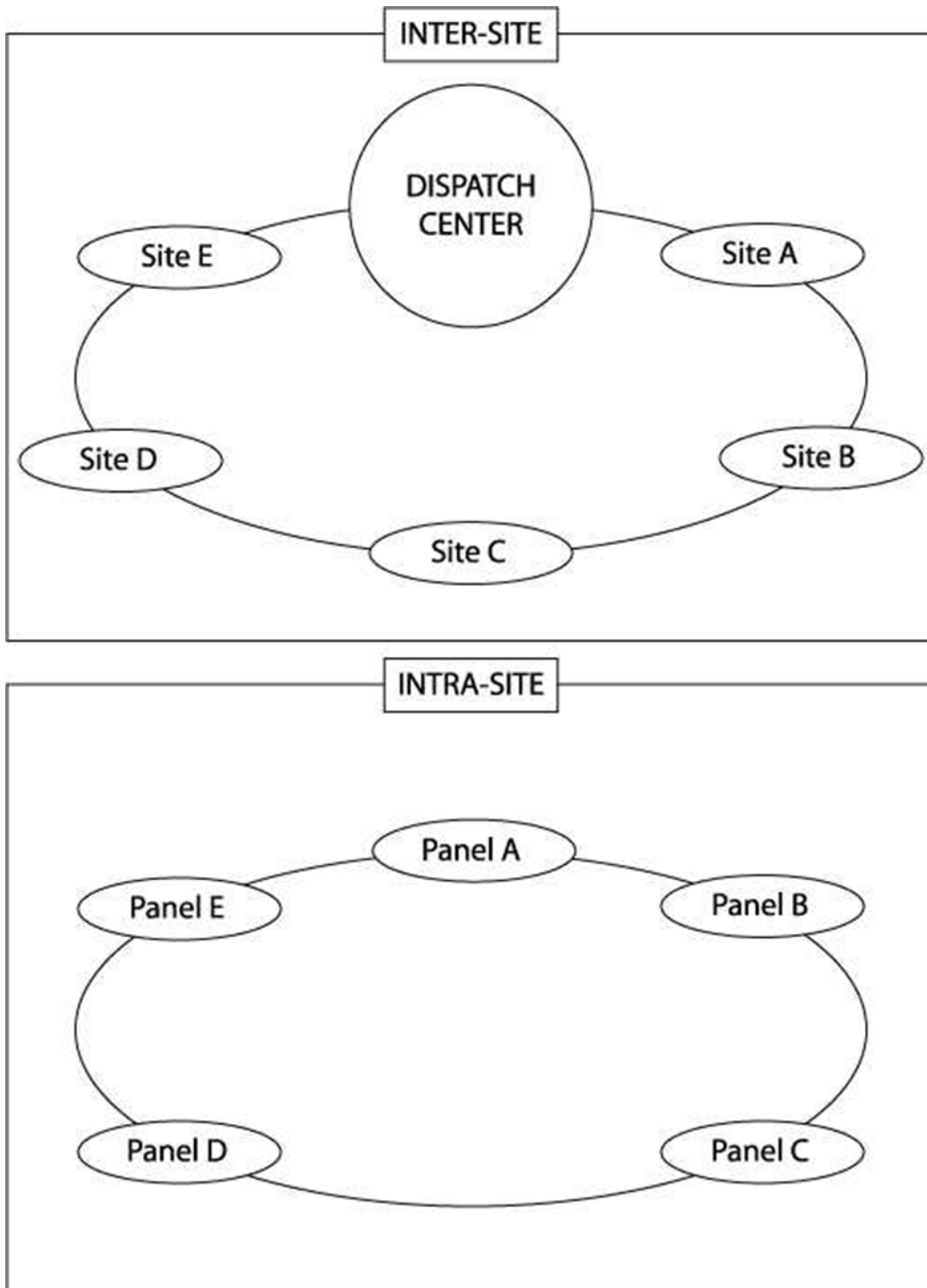
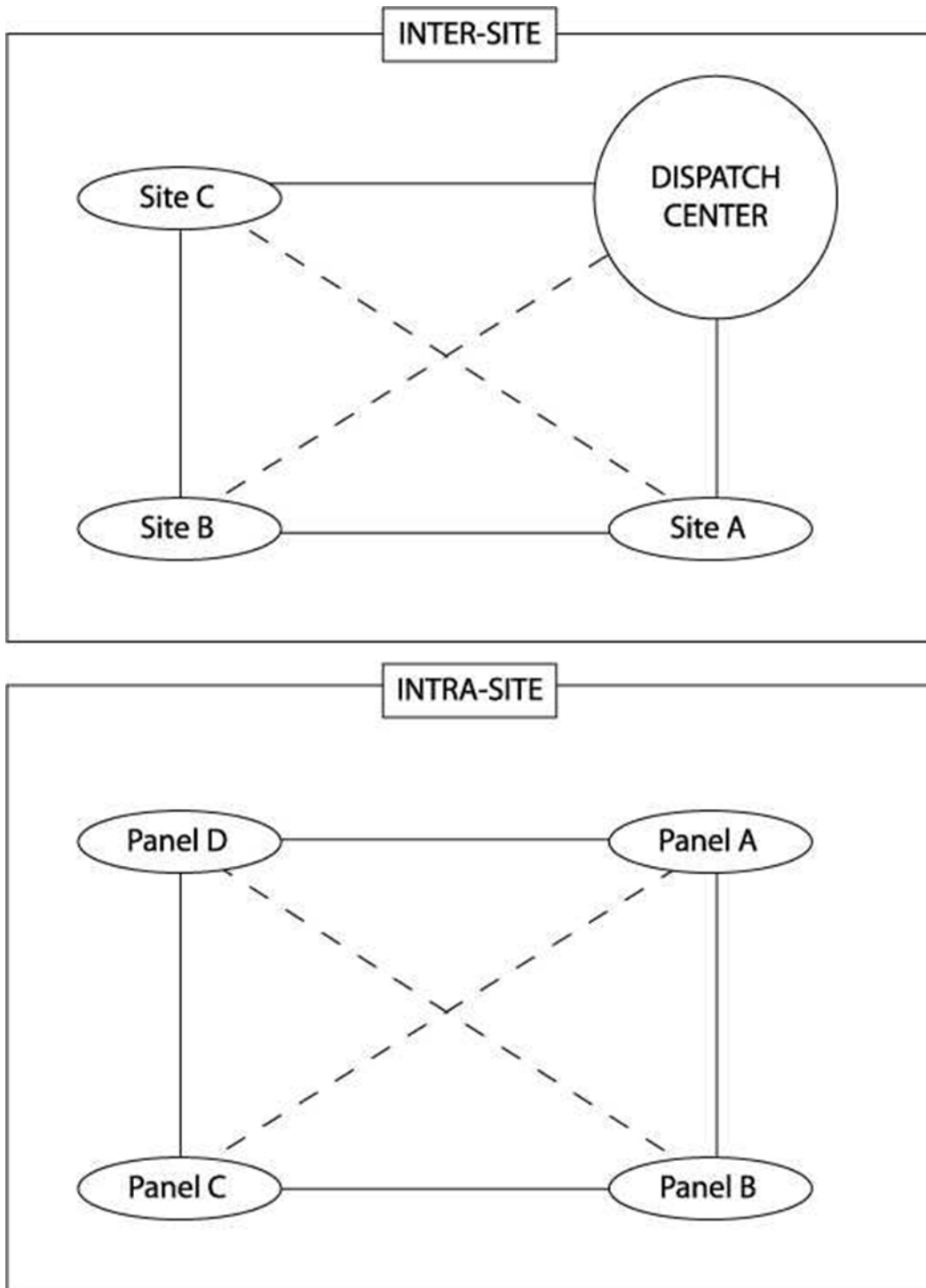


Figure 6-3. Fully-Meshed Topologies.



6-5 COMMUNICATION REDUNDANCY.

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 running primary as well as backup RS-485 lines. If this is done, it is best to use different raceway routing schemes.

New product developments and improved design configurations increasingly harden communication system redundancy. This concept is generally more applicable to network backbones 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.

Several modes and protocols exist for electronic security data transmission including serial communication (RS-485, RS-232), network communication using Ethernet protocol, modem, and wireless. The designer must consider protocol compatibility as well as data rate and distance requirements when selecting the appropriate data transmission methods for a project. The information presented in Table 6-2 will aid in this selection process. This information is discussed in the following section as part of an overview of the data transmission media commonly specified for ESS projects.

6-7 TRANSMISSION MEDIA.

6-7.1 Hardwired.

Hardwired refers to using dedicated proprietary (DoD-owned) circuits to transmit data/video between DTM nodes. Dedicated circuits can be copper or fiber-optic, both of which are discussed below.

6-7.1.1 Copper Circuits.

Copper circuits can meet most ESS data transmission needs from alarm circuits transmitting a simple state change to network links operating at speeds up to 1 Gb/s. As shown in Table 6-2, copper circuits are capable of supporting lower data rates out to distances of 1,000 feet (305 m) and greater, but copper Ethernet links can be no longer than 330 feet (100 m). Single-pair high-speed digital subscriber line (SHDSL) technology is a good option for achieving moderately high data rates at fairly long distances over a single copper pair. Disadvantages of copper circuits include susceptibility to electromagnetic interference, radio-frequency interference and damage from lightning strikes.

6-7.1.2 Fiber Optic Cable.

Fiber optic allows transmission over longer distances by using light, which does not have the higher resistance loss over distance of copper circuits. Furthermore, fiber optic is not affected by electromagnetic interference or lightning. As seen in Table 6-2, fiber

optic cable, when compared to copper, allows high data rate links to be established over much greater distances. For example, a Gigabit Ethernet link of 6.2 miles (10,000 m) is possible with fiber, compared to only 330 feet (100 m) with copper. Since the cost of a data transmission system can be a significant component of overall ESS cost, the designer must evaluate the advantages of fiber links in light of their higher cost compared to copper circuits. Of the two varieties of fiber optic cable, single-mode fiber offers greater distance capabilities than multi-mode fiber but is more expensive to implement.

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 point-to-point link.

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). 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 Wireless Security

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.

6-7.3.2 Frequency Allocation.

Frequency allocation or radio frequency spectrum planning is a critical issue and must be an early project design consideration. Frequency allocation is a long lead-time item. Employment of radio frequency transmitting equipment outside of the continental United States may require approval by the Host nation. Refer to service policies for frequency allocation.

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 cable. FSO systems can function over distances of several kilometers, but each link requires 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.

Table 6-2. Data Transmission.

Protocol / Media	Data Rate @ Distance
Supervised alarm circuit / copper, single pair	state change @ 1,000 feet (305 m)
RS232 / copper	19.2 kb/s @ 50 feet (15 m)
	9.6 kb/s @ 500 feet (150 m)
	4.8 kb/s @ 1,000 feet (300 m)
	2.4 kb/s @ 3,000 feet (900 m)
V.35 / copper	1.5 Mb/s @ 50 feet (15 m)
	56 kb/s @ 102 feet (31 m)
	19.2 kb/s @ 513 feet (156 m)
	9.6 kb/s @ 1,025 feet (312 m)
	4.8 kb/s @ 2,050 feet (625 m)
	2.4 kb/s @ 4,100 feet (1250 m)
RS422 / copper	10 Mb/s @ 40 feet (12 m)
	1 Mb/s @ 200 feet (61m)
	100 kb/s @ 4,000 feet (1220 m)
RS485 / copper	10 Mb/s @ 40 feet (12 m)
	1 Mb/s @ 200 feet (61m)
	100 kb/s @ 4,000 feet (1220 m)
SHDSL / copper, single pair	256 kb/s @ 21,980 feet (6,700 m)
	1.5 Mb/s @ 16,404 feet (5,000 m)
	2.3 Mb/s @ 13,780 feet (4,200 m)
10BASE-T Ethernet / copper, two pairs	10 Mb/s @ 328 feet (100 m)
Fast Ethernet / copper, two pairs	100 Mb/s @ 328 feet (100 m)
Fast Ethernet / multi-mode fiber, two fibers	100 Mb/s @ 1,804 feet (550 m)
Fast Ethernet / single-mode fiber, two fibers	100 Mb/s @ 32,808 feet (10,000 m)

Gigabit Ethernet / copper, four pairs	1 Gb/s @ 328 feet (100 m)
Gigabit Ethernet / multi-mode fiber, two fibers	1 Gb/s @ 1,804 feet (550 m)
Gigabit Ethernet / single-mode fiber, two fibers	1 Gb/s @ 32,808 feet (10,000 m)

6-8 TECHNOLOGY COMPARISON.

Table 6-3 provides a comparison matrix of different DTM technologies for ESS.

Dedicated conductors are highlighted 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 data rate and distance requirements.

6-9 ENCRYPTION.

An ESS designer is responsible for reviewing applicable security policies and consulting with information assurance (IA) personnel to determine data transmission encryption requirements and methods on a project-by-project basis. Two details must be addressed when making this determination - the types of data being transmitted and the data transmission techniques being used. As a general guideline, ESS data associated with very high security assets (such as SCIFs) or containing personally identifiable information (such as biometrics) must be encrypted. Encryption will generally be required when any ESS data is transmitted using techniques such as wireless links and shared or public networks that are inherently more susceptible to interception than hardwired circuits and closed, restricted ESS networks.

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

Table 6-3. 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 have 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.	Reasonable alternative to "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 and encrypted.	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 and shutdown network.

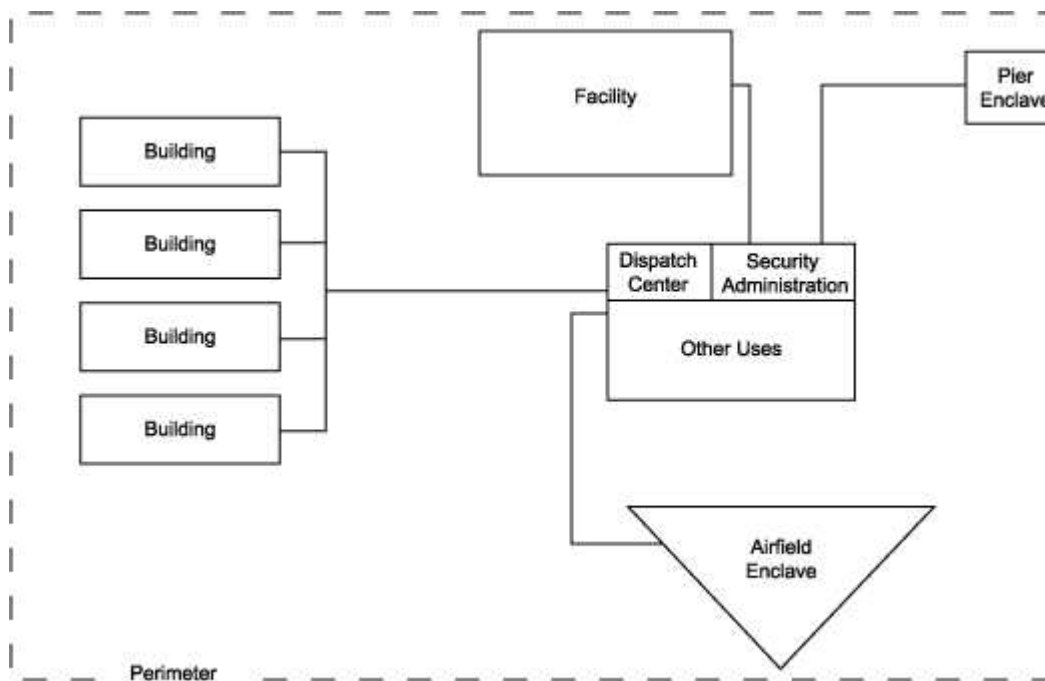
CHAPTER 7 DISPATCH CENTER

7-1 INTRODUCTION.

7-1.1 Dispatch Center.

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. The Dispatch Center must meet the applicable requirements of NFPA 1221. 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.

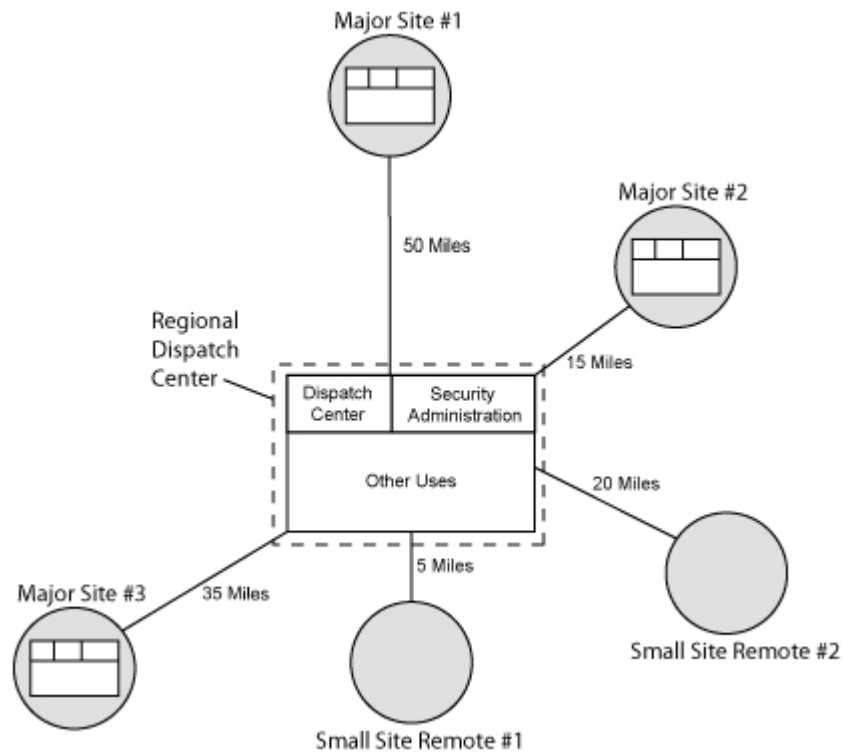
Figure 7-1. Dispatch Center Centrally Located.



7-1.2 Regional Dispatch Center (RDC).

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 Facility Options.

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.

Space programming for a Dispatch Center must consider the following:

- a. Equipment wall space
- b. Provide a minimum 36 inches (900 mm) space both in front and in back of equipment racks and a minimum side clearance of 24 inches (600 mm) on end equipment racks.
- c. Counter space for consoles
- d. Personnel space for each operator
- e. Space for UPS equipment
- f. Access requirements for maintenance or repair.
- g. Conduit space requirements for future system wiring or enhancements.
- H. Future growth or expansion space

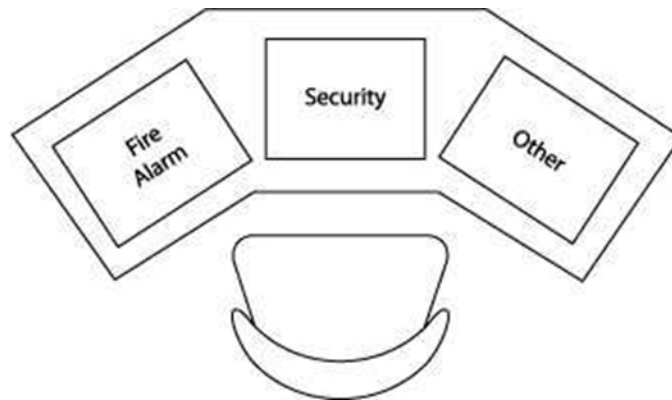
7-3 LIGHTING.

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 must be given to selectable lighting or dimmers that allow reducing the lighting behind or near system displays. Use of dimmers or task lighting must be considered at operator's areas. Indirect lighting should be a consideration. The design should strive for no glare on monitor screens.

7-4 CONSOLES.

A determination should be made early as to how many consoles 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.

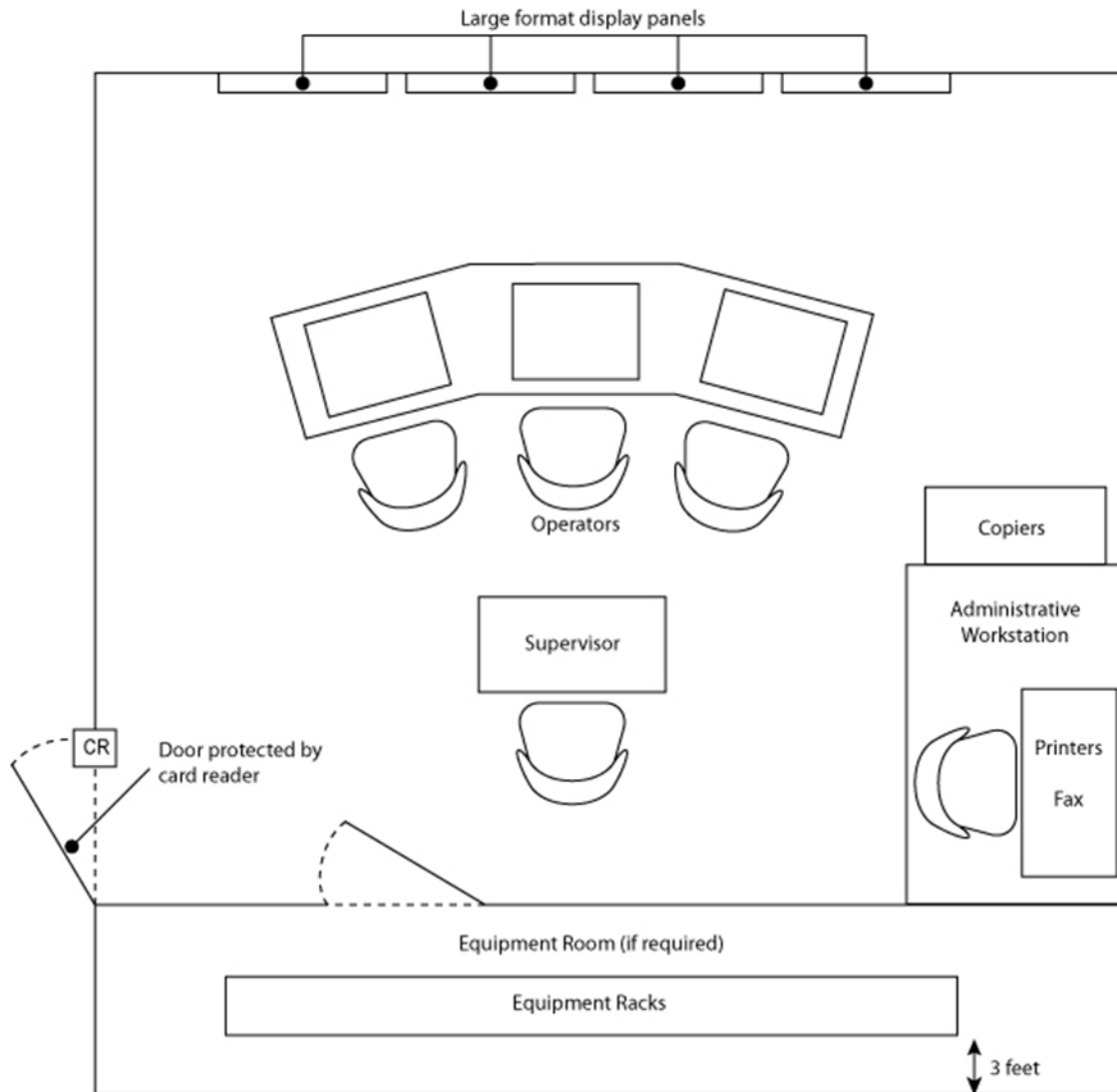


7-5 MONITORS.

Monitors must be ergonomically mounted. Current products allow wall-mounted flat-screen displays and smaller, hinged, flat-panel monitors that can be swiveled out and adjusted for individual operators.

The quantity, size, and resolution of monitors are all important design considerations, with the primary goal being to maximize the effectiveness of operators in performing their duties. For a single-operator workstation, two to four monitors is generally adequate, recognizing that more is not necessarily better. Monitors in the 20 - 24-inch (500 – 600 mm) display range providing HD 1080p resolution are a good, economical option for most ESS applications.

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



7-6 GROUNDING/POWER CONDITIONING.

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 ANSI/TIA-J-STD-607 for additional guidance on grounding, surge protection, and power conditioning.

7-7 HEATING, VENTILATION AND AIR CONDITIONING.

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.

7-7.1 Environmental Considerations.

Typical environmental conditions for a Dispatch Center are as follows:

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

7-7.2 Load Calculation Considerations.

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

- a. 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 must all be considered when calculating this heat load component. For personnel, ASHRAE 62.1 recommends 20 cfm (9.4 l/s) flow rate per occupant. Refer to UFC 3-501-01 and utilize equipment loads based on the room configuration.
- b. Shell Load. Shell load considers the perimeter walls, ceilings, windows, and associated solar gains of the external surfaces.
- c. Outside Air. This load component varies according to the climatic conditions of the Dispatch Center location.

7-7.3 Components Considerations.

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

7-8 SUPPORT ROOMS.

A good practice is to plan for space in a room near the Dispatch Center to house support equipment. 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.

This Page Intentionally Left Blank

CHAPTER 8 ESS SUBSYSTEM INTEGRATION

8-1 OVERVIEW.

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.

As covered in Chapter Two, "Electronic Security System (ESS) Overview," for an intermediate system, the IDS may already be an integral part of the ACS. In these 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.

For some facilities, however, the IDS and ACS will be separate. This is a fairly common scenario in which each IDS zone within a facility is equipped with an IDS local processor connected to the Dispatch Center for the sole purpose of IDS alarm monitoring, and doors/portals within the facility are controlled by a local ACS administered and monitored by the owner/tenant. In facilities where the two systems are separate, the IDS and ACS often share a common need to monitor the position of certain doors. Rather than having two position sensors on a door (one for IDS and the other for ACS), the designer should specify a single door sensor that has two independent outputs. This allows one output to be wired to the IDS local processor and the other to the ACS local processor. This approach reduces the cost and eliminates the clutter associated with having two sensors on a single door.

8-3 COMMUNICATION FROM THE IDS¹ TO THE CCTV SYSTEM.

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 operator's attention.

8-3.1 Hardwired Conductors.

This is older technology, but it is still effective for simple installations. In this case, copper wiring is taken as digital outputs from the IDS or combined ACS/IDS and

¹ or combined ACS/IDS

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.

8-3.2 Serial Communications.

In theory, this is the same principle of operation as the hardwired method with an improvement in that a single serial data link can handle several camera control 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 if appropriate software drivers are available. While slightly more complicated than the hardwired approach, this method has the advantage of reduced wiring costs.

8-3.3 Software-Based Integration for Networked ESS.

This approach provides flexibility in the initial system setup and allows the user to make configuration changes via software with no additional hardware or wiring investment. For this reason, software-based integration is preferred for most projects, but it requires a networked ESS in which all subsystems are connected to a common IP network. In this approach, all file servers, workstations, video recording devices, cameras, and local processors are connected to the same network via Ethernet cables and switches. This network configuration 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 has to be the same vendor unless compatible software drivers for allowing both systems to talk to each other are available.

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

Cameras may be used to visually assess access control alarms in the same way they are used to assess intrusion alarms. Cameras may also be used to visually confirm the identity of a person requesting entry into a secure area before releasing the portal (referred to as video verification by some ACS vendors). The IDS/CCTV integration techniques described above also apply to ACS/CCTV integration.

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

ACS alarms may be transmitted from a facility to the Dispatch Center. The designer must determine for each project whether a facility owner/tenant will monitor ACS alarms locally or will rely on the Dispatch Center to provide ACS monitoring services. If the

Dispatch Center will monitor ACS alarms, the monitored facility must be equipped with a local processor that is compatible with the existing central monitoring system.

8-6 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).

This Page Intentionally Left Blank

CHAPTER 9 GENERAL CONSIDERATIONS AND CROSS-DISCIPLINE COORDINATION

9-1 GENERAL CONSIDERATIONS.

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:

- All local processors should be located within the secure area.
- Annunciators, controls and displays subsystems should be located in areas closed off from public access or view.
- Certifications and Listings.

9-1.1.2 Equipment and Systems.

Equipment and systems should be proven with a demonstrated history of reliability. One way of achieving this criterion is to specify listed or certified products/systems such as:

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

9-1.1.3 Spare Capacity.

An ESS must 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.

9-1.2 System Acceptance Testing.

The ESS technical specifications or scope of work must include requirements for the ESS installation contractor to conduct comprehensive testing of every component and feature in order to demonstrate acceptable system performance to the Government. This section discusses system testing and ownership acceptance procedures.

9-1.2.1 Labeling.

Major equipment must have labels to identify the system and device. Cables must be labeled at origination, termination, and within enclosures using permanent labels.

9-1.2.2 Test Documentation and Acceptance Forms.

The ESS installation contractor must prepare a test plan along with detailed test procedures and submit these to the Government for approval prior to testing. The ESS designer must include this requirement in the technical specifications or the Scope of Work.

9-1.2.3 Pre-Test Walkthrough.

A pre-test walkthrough should be performed just prior to the start of the final acceptance testing. This allows the final acceptance test to go smoothly and prevents mishaps and additional testing. The walkthrough also provides a good opportunity to check installation workmanship and validate equipment types and quantities against the design requirements. The designer should participate in the walkthrough along with the installation contractor and the Government representative.

9-1.2.4 Training.

Include administrator and operator training and add the number of hours required to the 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 must be able to unilaterally make additions or deletions to the ACS database.”

9-1.3 Operation and Maintenance.

In specifying ESS, the designer must consider maintenance, service, repair, and sustainability of systems and the associated components. Systems with arduous requirements should be reconsidered.

9-2 GENERAL COORDINATION.

Throughout the planning and design process the designer must coordinate closely with security (Physical Security Officer) and anti-terrorism personnel (Antiterrorism Officer), end-users, base communications officer (information technology and information assurance), fire and safety personnel, and the installation facilities engineering office.

9-3 CIVIL COORDINATION.

9-3.1 Gate Control (Vehicle Gates and Sally Ports).

A sally port is a secure controlled entry and exit portal, utilized for inspections and to prevent tailgating. Sally ports may require control hardware for interlocking gates. Refer to UFC 4-022-01 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 coordinate with existing civil drawings and buried utilities.

9-3.3 Outdoor Perimeter Security Features.

Perimeter security projects often involve clearing, grading, drainage improvement, erosion control and paving, and these design elements must be coordinated with local site development and environmental representatives. Civil Engineering input must be solicited when designing above-ground perimeter security features such as fences, passive vehicle barriers, towers, and poles.

9-4 ARCHITECTURAL COORDINATION.

Past experience shows that the biggest disconnect in project design and a construction cost 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 must be conducted during design development and creation of construction documents.

9-4.1 Balance of Security with Convenience.

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.

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 must not be sacrificed for convenience. Proper security controls will reduce the flow rate and ease of ingress and egress for a facility. These issues must be addressed in initial planning to facilitate additional entry points or administrative requirements.

9-4.1.1 Entries and Exits.

In general, provide separate entries and exits. Establish the number of entry/exit points consistent with security and Life Safety requirements.

9-4.1.2 Space Planning.

Early in the project, architectural issues for Dispatch Center space, wall space for security panels and floor space for ESS equipment racks and consoles need to be discussed. Normally, security panels will go in telecommunication rooms. The ESS designer must coordinate with the telecommunications system designer and local Information Technology personnel for space requirements in the telecommunications room.

DoD criteria require that telecommunication rooms are separate from electrical equipment rooms. These spaces will be climate controlled separately from adjacent spaces.

9-4.1.3 Doors.

Access 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 opened from the “public-side.”

9-4.1.3.1 Fail-Safe.

Fail-safe doors fail unlocked 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.

9-4.1.3.2 Fail-Secure.

Fail-secure refers to entry from the public-side. Fail-secure doors fail locked 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).

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.

9-4.1.4 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 must be an early design consideration 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.

9-4.1.5 Door Locks.

9-4.1.5.1 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 the top of the door and an additional retractable bolt on the side). 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. In addition to the lock itself, a special door hinge and internal are required. For retrofit applications, electric locks usually require purchase of a new door.

9-4.1.5.2 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 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.

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 or screwdriver.

9-4.1.5.3 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, which may be a problem for unstaffed facilities in that a power disruption that will leave the site unsecured until security personnel arrive or power is restored. Magnetic locks should be the designer's last choice for door locking mechanisms and should only be considered on a retrofit project.

Magnetic locks do have a security disadvantage. In the United States, life safety requirements generally favor the use of a passive infrared (PIR) sensor as the primary request-to-exit (REX) device for doors equipped with magnetic locks. While enhancing

overall building safety, this configuration in which a REX PIR sensor is mounted above the secure side of the door allows possible compromise of the magnetic door lock in the following scenario:

- Person A is on the secure side and walks past the door with no intent to exit
- The magnetic lock is released by the activation of the REX PIR sensor. This activation generates a "click" sound.
- Person B is on the public side of the door and, upon hearing the "click", opens the unlocked door and enters the secure area.

9-5 LIFE SAFETY CODE COORDINATION.

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 fire protection engineer (for items such as exit plan considerations and fire alarm system integration) to implement security without comprising life safety code standards. Physical security system designs need to be coordinated with and comply with NFPA 101 and the *ABA Accessibility Standard for Department of Defense*.

9-6 ELECTRICAL COORDINATION.

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.

9-6.1 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.

9-6.2 Backup Power.

9-6.2.1 Battery Backup.

The minimum requirement for battery backup for an IDS and its monitoring station is eight hours². This may be provided by batteries integral to the IDS, uninterruptible power supply (UPS), or generators, or any combination. Emergency backup power for IDS will not generate the requirement for a UPS or generator. If a generator or UPS is not available for backup, provide backup with batteries.

² Based on DoD O-2000.12-H, Antiterrorism Handbook

In the event of primary power failure, the IDS must:

- Automatically transfer to an emergency electrical power source without causing alarm activation.
- Initiate an audible or visual indicator at the PCU to provide an indication of the primary or backup electrical power source in use.
- Initiate an audible or visual indicator at the monitoring station indicating a failure in a power source or a change in power source.

9-6.2.2 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. Backup power must be provided for CCTV systems that employ video analytics as the primary means of intrusion detection and considered when used for surveillance around critical assets.

9-6.3 Grounding, Bonding, and Lightning Protection.

Refer to UFC 3-520-01 Interior Electrical Systems, UFC 3-575-01, ANSI/TIA J-STD-607, NFPA 70, and NFPA 780 as applicable.

9-6.4 Cable Type.

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, and capacitance) time constants. The ESS designer should specify low capacitance cable and sufficient twists per foot that meet manufacturers’ specifications.

9-6.5 Surge Protection.

Provide surge protective devices for all systems identified in NFPA 780. Refer to UFC 3-520-01 for the requirements.

9-6.6 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.

9-6.7 Tamper Protection.

Tamper protection for ESS can be physical protection, line supervision, encryption, and/or tamper alarming of enclosures and components. \1\ /1/ All tamper alarm signals

must be monitored continuously whether the system is in the access or secure mode of operation.

9-6.7.1 Cable Routing.

All conduit and cabling associated with the ESS should be installed within the perimeter of the protected area to the greatest extent possible. A communications link from a protected area to a central monitoring system is an obvious exception to this guideline.

9-6.7.2 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, workstations, and the associated central system. 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. DTM supervision must initiate an alarm upon any manipulation or disruption of the signal.

9-6.7.3 Encryption.

Encryption provides a level of protection against interception and malicious use of ESS data associated with high-security facilities and personally identifiable information. In general, encryption must comply with NIST FIPS standards. Refer to specific service policy for the asset being protected.

9-6.7.4 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 the following methods:

- In rigid or intermediate metal conduit as defined by NFPA 70.
- In concrete encased duct.
- In conduit buried a minimum of twenty-four inches (0.6 meters) below finished grade.
- Suspended at a minimum of 15.5 feet (4.5 meters) above the finished grade.

9-6.7.5 Physical Protection of Interior ESS.

All intrusion detection sensors, access control readers, and assessment equipment located outside controlled areas must have tamper resistant enclosures. All interior intrusion detection sensors and access control readers must have integral tamper protection switches. All ESS cabling should be routed within the protected area to the greatest extent possible. Additionally, the following design criteria must be applied:

- a. All enclosures, cabinets, housings, boxes, and fittings having hinged doors or removable covers must be locked, welded, brazed, or secured with tamper resistant security fasteners and be tamper-alarmed.
- b. Any metallic conduit that leaves an area that processes classified information such as a SCIF must be decoupled (insert of nonmetallic conduit) when exiting the area.
- c. For ordnance facilities, metallic conduit must be run underground for at least 50 feet (15 m) from the structure. Refer to UFC 3-575-01 for additional requirements.
- d. Comply with applicable security policy requirements for installing IDS communications wiring in conduit. Apply security policy for the specific asset being protected. For example, security policy for SCIFs requires: "IDS-associated cabling that extends beyond the SCIF perimeter must be installed in rigid conduit or must employ line security". There is no universal requirement for IDS wiring to be installed in conduit.

9-6.8 Radio Frequencies.

RF systems must employ some form of tamper protection such as:

- The security system must use dedicated frequencies to transmit ESS alarm data.
- The system must detect and report intentional and unintentional jamming attempts.

9-6.9 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 must strive for a voltage drop of 10% or less.

9-6.10 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).

9-6.10.1 In a Power System

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.

9-6.10.2 Mitigation

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.

9-6.10.3 Electrical Noise Reduction

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.

9-6.11 Raceway.

All conduit, wireway, and raceway must meet the requirements of NFPA 70.

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

9-6.12 Labeling.

Cables must be labeled at origination, termination, entry into and exit from enclosures with permanent labels.

9-6.13 Shielding.

When required, shielded cable must only be grounded at one end, typically back at the local security panel to prevent open loop grounds.

9-6.14 Fire Alarm System.

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, hospitals, and other high security facilities.) Methods vary on how this may be accomplished. Meet

requirements of NFPA 101. 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. The ESS design needs to include the elements identified in Figure 9-1 for system interface.

Figure 9-1. 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.

9-6.15 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.

9-6.16 Lighting.

While not an official part of ESS, lighting is an effective part of the overall physical protection design, see UFC 3-530-01. Lighting may 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.

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.

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

- Material entry control circulation should be separated from general facility traffic.
- Loading docks are typically monitored by fixed cameras.
- Rollup doors are normally monitored by an interior point sensor such as a BMS.
- 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.

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.

Two principle 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.

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

10-2.1 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.

10-2.2 Existing Site and Building Plans.

Locating and obtaining site plans and building plans for associated buildings should be accomplished during the planning stage. CAD drawings are preferred. Early in the design process, the ESS designer should conduct site surveys to verify the accuracy of the existing plans with regard to current site conditions.

10-2.3 Site Surveys.

Site surveys include a capacity assessment of existing systems to include the following issues:

- a. ACS: How many spare card reader slots are available at what panels?
- b. What type of credential is used?
- c. Is there badging (issuing new badges) capability?
- d. CCTV: How many spare camera ports back at central server?
- e. Is archiving capability present?
- f. IDS: any expansion capability?

- g. Transmission system bandwidth availability.
- h. Approval of radio frequency emitters by local jurisdiction or host nations
- i. Coordination of DTM transmission Lines

For existing and new DTM transmission lines, coordinate with the base communications officer (information technology).

10-2.4 Dispatch Center.

Identification of the location of the central monitoring facility (space) for the ESS must 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 refer 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.

10-2.5 Multi-Organizational Interfaces.

Meetings with end users and facility security specialists need to be held. Additionally, determine facility and security forces operational requirements.

10-2.6 Space Planning.

The ESS designer must interact early to reserve space requirements in a new building (square footage area) for ESS components such as equipment racks, consoles, operator stations, and administrative stations.

10-3 INITIAL DRAWING PREPARATION.

A good start for drawing production is to begin with security plan drawings and a system block diagram.

10-3.1 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. This approach is illustrated in Figures 10-1 and 10-2.

Figure 10-1 Cable Counts on Riser Diagrams.

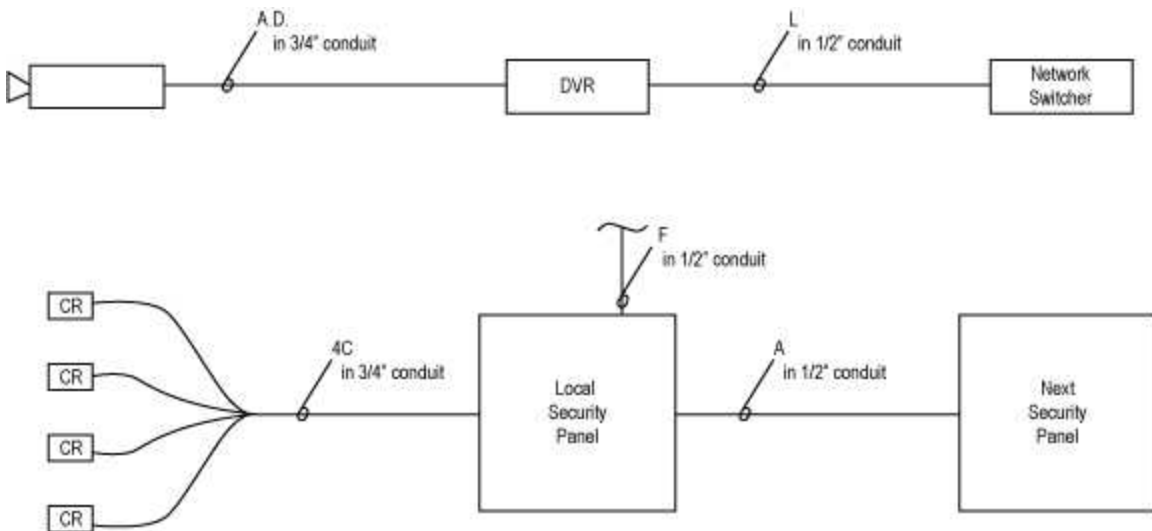


Figure 10-2. Sample Cable Schedule.

Cable Legend	Style	Type	Use
A	#16/1 TSP	Communication Cable Plenum Rated (CMP)	RS-485
C	#20 AWG/ 3 TSP	Communications Cable 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 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

10-3.2 Functional Matrix.

A document defining the functionality to the system is a useful tool similar to the one, and an example shown in Figure 10-3.

10-4 BASIS OF DESIGN.

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 10-3. Functional Matrix.

ACTION		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 PT Z camera "moves" to preset location Door unlocks until fire alarm panel is reset Motorized gate opens Response force mobilized									
		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.

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.

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.

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

- Legends and abbreviations
- Site plans
- Floor plans
- Riser diagrams
- Mounting details
- Door hardware schedule (may be on architectural plans)
- Sequence of construction when applicable
- 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.

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

10-7 BIDDING.

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.

This Page Intentionally Left Blank

APPENDIX A REFERENCES

AMERICAN SOCIETY OF HEATING, REFRIGERATION, AND AIR CONDITIONING ENGINEERS

<http://www.ashrae.org/>

ASHRAE 62.1, *Ventilation for Acceptable Indoor Air Quality*

ASIS INTERNATIONAL

<http://www.asisonline.org/Pages/default.aspx>

Effective Physical Security, 4th Edition, Lawrence J. Fennelly, Elsevier, Butterworth-Heinemann

IEEE

<http://www.ieee.org/index.html>

IEEE 519, *Guide for Harmonic Control and Reactive Compensation of Static Power Converters*

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

<http://www.iso.org>

ISO/IEC 14443, Part 1, *Identification Cards -- Contactless Integrated Circuit Cards -- Proximity Cards -- Part 1: Physical Characteristics*

ISO/IEC 14443, Part 2: *Identification Cards -- Contactless Integrated Circuit Cards -- Proximity Cards -- Part 2: Radio Frequency Power and Signal Interface*

ISO/IEC 14444, Part 3, *Identification Cards -- Contactless Integrated Circuit Cards -- Proximity Cards -- Part 3: Initialization and Anticollision*

ISO/IEC 14443, Part 4, *Identification Cards -- Contactless Integrated Circuit Cards -- Proximity Cards -- Part 4: Transmission Protocol*

SANDIA NATIONAL LABORATORIES

Design and Evaluation of Physical Protection Systems, Mary Lynn Garcia, Butterworth-Heinemann, Boston

NATIONAL FIRE PROTECTION ASSOCIATION

<http://www.nfpa.org>

NFPA 70, *National Electrical Code*

NFPA 101, *Life Safety Code*

NFPA 780, *Standard for the Installation of Lightning Protection Systems*

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

<http://www.nist.gov/index.html>

FIPS 201, *Standard for Personal Identity Verification of Federal Employees and Contractors*, <http://csrc.nist.gov/groups/SNS/piv/standards.html>

NISTIR 6887, *Government Smart Card Interoperability Specification*,
<http://csrc.nist.gov/publications/PubsNISTIRs.html>

TELECOMMUNICATION INDUSTRY ASSOCIATION

<http://www.tiaonline.org>

ANSI/TIA J-STD-607-A, *Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications*

UL LLC

<http://www.ul.com>

UL 294, *Access Control System Units*

UL 634, *Connectors and Switches for Use with Burglar-Alarm Systems*

UL 639, *Intrusion Detection Units*

UL 681, *Installation and Classification of Burglar and Holdup Alarm Systems*

UL 2050, *National Industrial Security Systems*

U.S. ACCESS BOARD

ABA Accessibility Standard for Department of Defense Facilities, <http://www.access-board.gov/ada-aba/aba-standards-dod.cfm>

U.S. AIR FORCE

AFI 31-101, *Integrated Defense*

AFI 31-401, *Information Security Program Management*

U.S. ARMY

AR 190-11, *Physical Security of Arms, Ammunition, and Explosives*

AR 380-5, *Information Security Program*

Perimeter Security Sensor Technologies Handbook, Space and Warfare Systems Center, for the Defense Advanced Research Projects Agency Joint Program Steering Group,

<http://apps.hnc.usace.army.mil/esc/images/Documents/Perimeter%20Security%20Sensor%20Technologies%20Handbook.pdf>

U.S. DEPARTMENT OF DEFENSE

DoD Manual 5100.76, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)*, Department of Defense, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division, <http://www.dtic.mil/whs/directives/>

DoD Manual 5105.21, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division, <http://www.dtic.mil/whs/directives/>

DoD Manual 5200.01, *DoD Information Security Program: Protection of Classified Information*, Department of Defense, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division, <http://www.dtic.mil/whs/directives/>

DoD 5200.8-R (DTM) 08-004, *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 O.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/>

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, Assistant Secretary of Defense for Networks & Information Integration, Department of Defense, Washington Headquarters Service, Executive Services and Communication Directorate, Directives and Records Division, <http://www.dtic.mil/whs/directives/>

Intelligence Community Standard (ICS) 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, Office of the Director of National Intelligence

JAFAN 6/9, *Physical Security Standards for Special Access Program Facilities*, Joint Air Force - Army – Navy Manual

U.S. DEPARTMENT OF DEFENSE, UNIFIED FACILITIES PROGRAM

http://www.wbdg.org/references/pa_dod.php

UFC 1-200-01, *General Building Requirements*

UFC 3-501-01, *Electrical Engineering*

UFC 3-520-01, *Interior Electrical Systems*

UFC 3-530-01, *Design: Interior and Exterior Lighting and Controls*

UFC 3-575-01, *Lightning and Static Electricity Protection Systems*

UFC 4-010-01, *Minimum Antiterrorism Standards for Buildings*

UFC 4-010-02, *Minimum Antiterrorism Standoff Distances for Buildings* (FOUO)

UFC 4-010-05, *Sensitive Compartmented Information Facilities Planning, Design, and Construction*

UFC 4-020-01, *DoD Security Engineering Facilities Planning Manual*

UFC 4-020-02, *Security Engineering Facilities Design Manual*, currently in Draft and unavailable

UFC 4-021-01, *Design and O&M: Mass Notification Systems*

UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*

UFC 4-022-03, *Security Engineering: Fences and Gates*; scheduled to replace MIL-HDBK-1013/10, *Design Guidance for Security Fencing, Gates, Barriers, and Guard Facilities*

U.S. MARINE CORPS

MCO 5530.14A *Marine Corps Physical Security Program Manual*

U.S. NAVY

MIL-HDBK-1013/10, *Design Guidance for Security Fencing, Gates, Barriers, and Guard Facilities*, (scheduled to be replaced by UFC 4-022-03, *Security Engineering: Fences and Gates*), http://www.wbdg.org/ccb/browse_cat.php?c=80

OPNAV INSTRUCTION 5530.13C *Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives*

SECNAV M-5510.36, *Information Security Program*

APPENDIX B GLOSSARY

B-1 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
CSA—Cognizant Security Authority
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
FIPS—Federal Information Processing Standards
FRR—False Rejection Rate
FOUO—For Official Use Only
HD—High Definition
HVAC—Heating, Ventilation, and Air Conditioning
HVR—Hybrid Video Recorder
IDE—Intrusion Detection Equipment
IDS—Intrusion Detection System
IP—Internet protocol
IR—Infrared
IVS—Intelligent Video Surveillance
LAN—Local Area Network
LCD—Liquid Crystal Display

MNS—Mass Notification System
NAR—Nuisance Alarm Rate
NIST—National Institute of Standards and Technology
NMCI—Navy/Marine Corps Intranet
NVR—Network Video Recorder
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
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
VMD—Video Motion Detection
WAN— Wide Area Network

B-2 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.

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 typically will house the Dispatch Center, which is the centralized location for receiving and assessing ESS alarms.

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). The CAC, a "smart" card about the size of a credit card, is the standard identification for active-duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to defense computer networks and systems.

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 (ACC).

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, 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 phenomenon 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 fewer 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. Numerous nuisance alarms can cause complacency.

Premise Control Unit (PCU). A PCU is an electronic device that continuously monitors the alarm status of local intrusion detection sensors and duress devices and transmits alarm conditions to a remote monitoring station. The PCU allows authorized personnel to place the alarm zone in an “armed” or “disarmed” state via a local keypad, credential reader or biometric device. The term “PCU” is generally synonymous with the terms “IDS local processor” and “intrusion panel”.

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.

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 National Intelligence.

Sensitive Compartmented Information Facility (SCIF). A facility capable of storing Sensitive Compartmented Information (SCI) material. Requirements for these facilities are defined in ICS 705-1.

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.

Video Analytics/IVS. Video Analytics, also known as IVS (Intelligent Video Surveillance) is the practice of using computers to automatically identify things of interest without an operator having to view the video. IVS consists of algorithms that detect movement or changes in live and recorded video to see whether the movement or changes mean a possible threat is about to occur or occurring. These algorithms work by examining each pixel of the video and putting together all the pixel changes. If many pixels are changing in one area and that area is moving in a direction, the software considers this to be motion. Depending on the policies and alerts you have setup, you will be notified of this motion or other actions can be automatically taken by the software such as motion tracking which follows the motion until it is no longer detected.

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

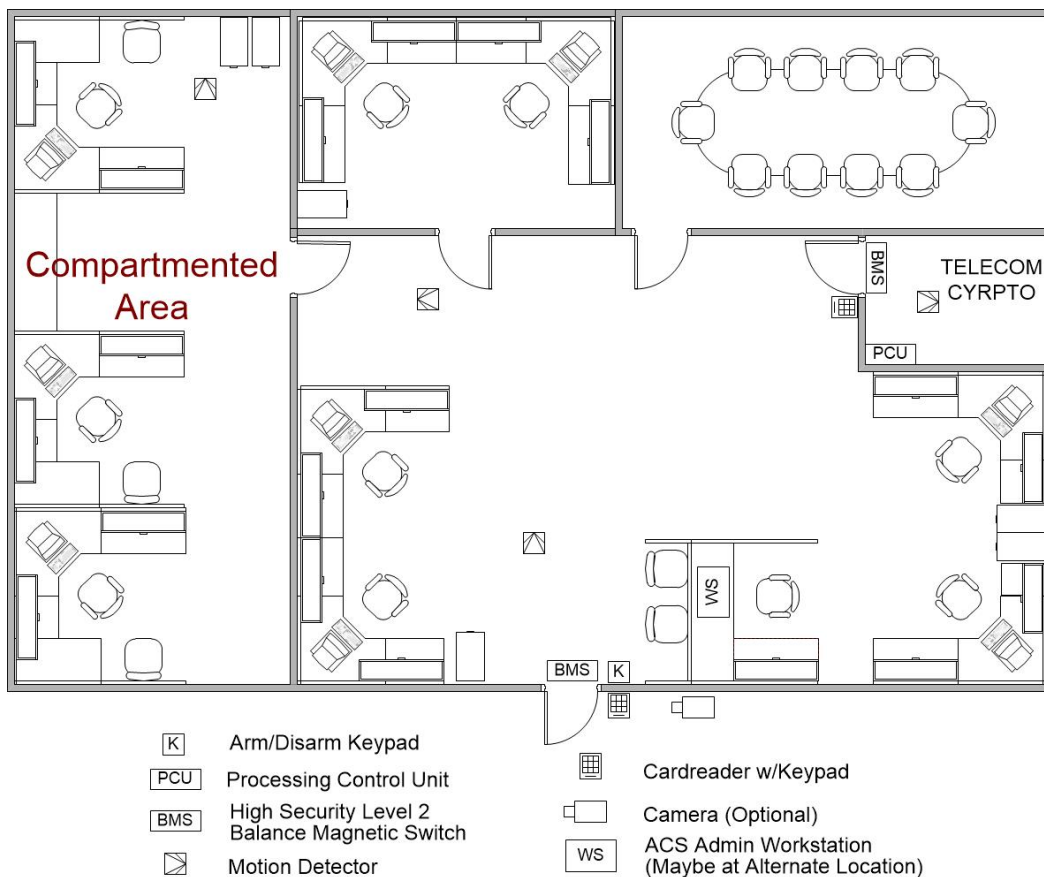
Acknowledgement: A computer dictionary called "Webopedia" was used for some of the definitions used in this glossary. Webopedia is found at <http://webopedia.com/>.

This Page Intentionally Left Blank

APPENDIX C NOTIONAL INTERIOR IDS CONFIGURATIONS

The information provided in this appendix is intended to aid the designer in understanding and applying policy-directed IDS requirements. It is not comprehensive as it addresses only a few high-security assets and summarizes only the most critical technical requirements. Using this information as a starting point, the designer must identify all security policies that pertain to each project and ensure that all IDS requirements are addressed in the design. \1\

C-1 SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF).



C-1.1 DoD Criteria Document.

UFC 4-010-05, Sensitive Compartmented Information Facilities Planning, Design, and Construction.

C-1.2 Policy Baseline.

- Director of National Intelligence, Intelligence Community Standard (ICS) 705-1 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities.

- DoD Manual 5105.21, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security.

C-1.3 Baseline Intrusion Detection System (IDS) Requirements.

- Must be protected by an IDS when not occupied.
- Provide point sensors on all doors, and man-passable openings. Provide motion sensors within SCIF to protect all windows, doors, and man-passable openings and detect movement within the SCIF to include compartmented areas.
- Emergency exit doors must be secured, alarmed, and monitored 24 hours per day.
- Interior areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the SCI level, must be protected by IDS consisting of motion sensors and Level 2 high security switches (HSS).
- IDS must be installed in accordance with UL 681 and consist of:
 - Point Sensors that meet UL 634 Level 2 high security switches (HSS). Level 2 rated switches only include Balanced Magnetic Switches that pass additional performance testing.
 - Motion detection sensors must be UL 639 listed. Dual-technology sensors may be used when authorized and when each technology transmits alarm conditions independent of the other technology (“or” configuration).
- Premise Control Units (PCUs) must be located within perimeter of a SCIF.

C-1.4 Cameras.

Cameras are not allowed within the SCIF.

C-1.5 Tamper Protection.

- All IDS systems; including any access control system equipment, must be equipped with tamper detection devices that must be monitored continuously whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU or monitoring station.
- IDS-associated cabling that extends beyond the SCIF perimeter must be installed in rigid conduit or must employ line supervision.
- All system sensors should be located within the perimeter of the SCIF. Cabling between all sensors and the PCU must be dedicated to the system, contained within the SCIF. With Accrediting Official (AO)

approval, sensors external to the SCIF perimeter and any perimeter equipment used may be connected to the IDS provided the lines are installed on a separate zone and routed within grounded conduit.

C-1.6 External Transmission Line Security.

- Any system transmission line that leaves a SCIF must have line supervision and be encrypted to National Institute of Standards and Technology FIPS 140-2. Alternative methods must be approved by the AO.

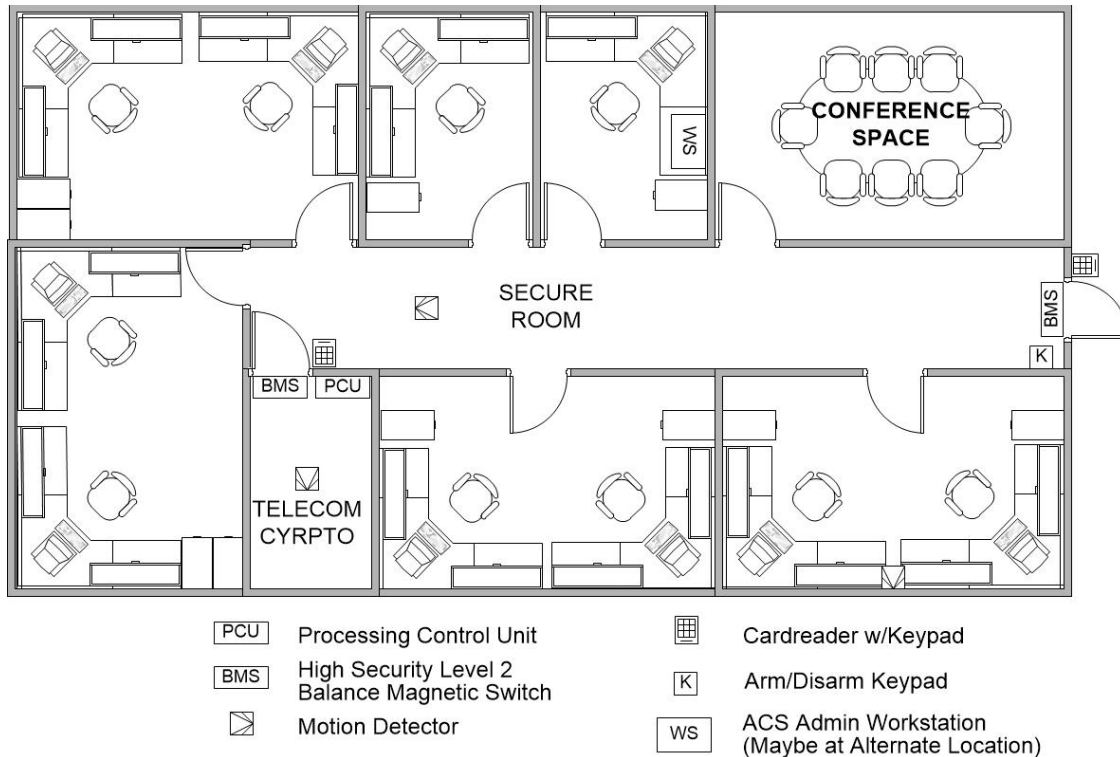
C-1.7 Emergency Backup Electrical Power.

- Twenty four hours of uninterruptible backup power is required. This may be provided by batteries integral to the ESS, uninterruptible power supply (UPS), generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.
- An audible or visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the monitoring station must visibly and audibly indicate a failure in a power source or a change in power source. The individual system that failed or changed must be indicated at the PCU or monitoring station as directed by the AO.

C-1.8 Optional Equipment.

- External CCTV Camera to monitor primary entrance.

C-2 SECURE ROOM (TOP SECRET OR SECRET OPEN STORAGE)



C-2.1 Policy Baseline.

- DoD Manual 5200.01, DoD Information Security Program: Protection of Classified Information
- SECNAV M-5510.36 Department of the Navy Information Security Program
- AFI 31-401 Department of the Air Force Information Security Program Management
- AR 380-5 Department of the Army Information Security Program

C-2.2 Baseline Intrusion Detection System (IDS) Requirements.

- Must be protected by an IDS when not continuously manned or under constant surveillance. If an IDS is not required, a continuously manned secure area should be equipped with an alerting system on all potential entrances into the secure area that cannot be observed by the occupants.
- All perimeter doors and man-passable openings into the secure area must be protected by High Security Switch (HSS) and a motion detection sensor.

- Keypad at Primary Entrance.
- Perimeter emergency exit doors must be secured, alarmed, and monitored 24 hours per day.
- IDS must be installed in accordance with UL 681 and consist of:
 - Level 2 high security switches (HSS) that meet UL 634, and/or other government approved sensors.
 - Motion detection sensors UL 639 listed. Dual-Technology Sensors are authorized when each technology transmits alarm conditions independent of the other technology.
- Premise Control Units (PCUs) must be located within a secure room.

C-2.3 Cameras.

Cameras are not allowed within spaces that contain classified materials.

C-2.4 Tamper Protection.

- All IDS systems, including any access control system connected must be equipped with tamper detection devices that must be monitored continuously whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU or monitoring station.
- System associated cabling that extends beyond the protected area perimeter must be installed in conduit and must employ electronic line supervision. Electronic line supervision will entail a polling or multiplexing system or equivalent. If line supervision is unavailable, two independent means of alarm signal transmission to the monitoring location must be provided.
- All system sensors must be located within the protected area.
- Cabling between all sensors and the PCU must be dedicated to the system, contained within the protected area.

C-2.5 External Transmission Line Security.

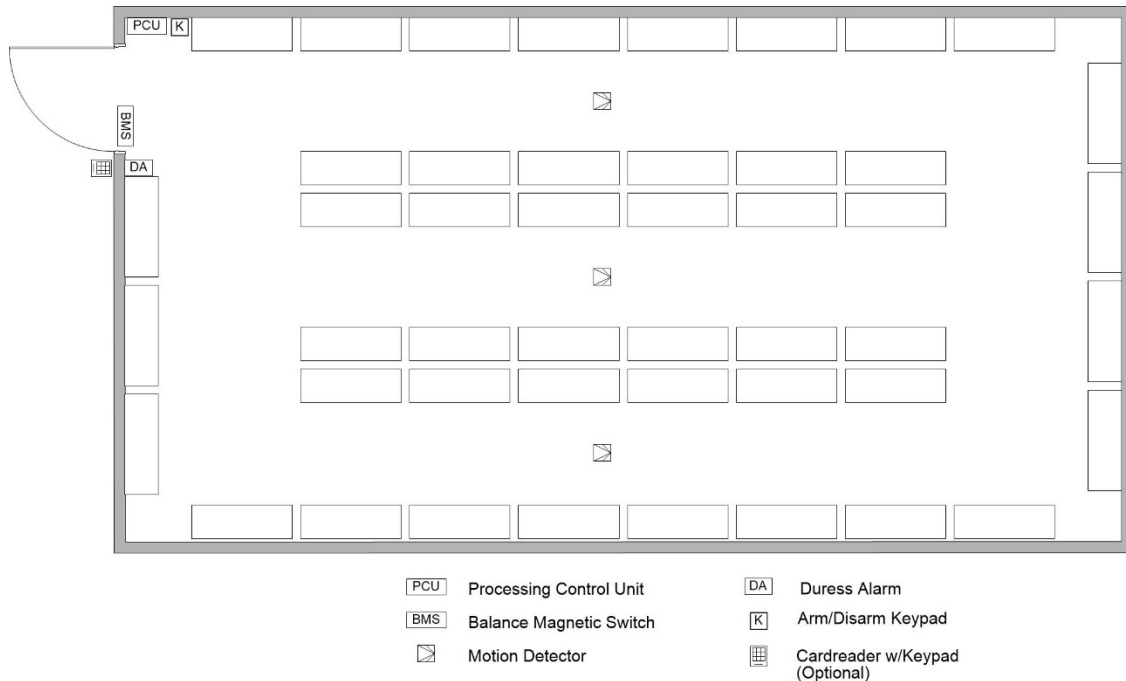
- Any system transmission line that leaves the protected area must be encrypted to National Institute of Standards and Technology FIPS 140-2.

C-2.6 Emergency Backup Electrical Power.

- Eight hours of uninterruptible backup power is required. This may be provided by an uninterruptible power supply (UPS), batteries integral to the ESS, generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.

- An audible or visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the monitoring station must visibly and audibly indicate a failure in a power source or a change in power source. /1/

C-3 ARMS STORAGE AREA (ARMORY, ARMS ROOM, READY ISSUE ROOM).



C-3.1 Policy Baseline.

- DoD Manual 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E),
- OPNAV INSTRUCTION 5530.13C Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives.
- MCO 5530.14A Marine Corps Physical Security Program Manual
- AFI 31-101 Department of the Air Force Integrated Defense
- AR 190-11 Department of the Army Physical Security of Arms, Ammunition, and Explosives

C-3.2 Baseline Intrusion Detection System (IDS) Requirements.

- Must be protected by an IDS when not continuously manned or under constant surveillance.

- All perimeter doors and man-passable openings into the storage area must be protected by High Security Switch (HSS) and a motion detection sensor.
- Duress alarm at all issue ports.
- Keypad at entrance and for all separated (unit-based) interior storage areas that require an independent IDS capability.
- Perimeter emergency exit doors must be secured, alarmed, and monitored 24 hours per day.
- IDS must be installed in accordance with UL 681 and consist of:
 - Level 2 high security switches (HSS) that meet UL 634, and/or other government approved sensors.
 - Motion detection sensors UL 639 listed.
- Premise Control Units (PCUs) should be located within the protected area.

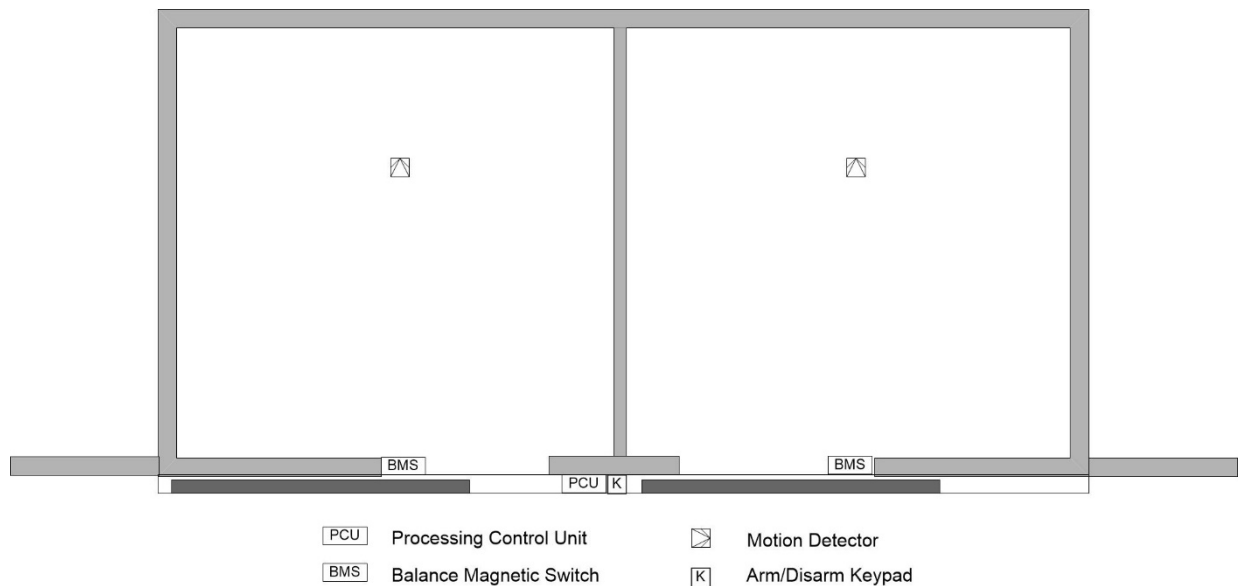
C-3.3 Tamper Protection.

- All IDS systems, including any access control system connected must be equipped with tamper detection devices that must be monitored continuously whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU or monitoring station.
- System associated cabling that extends beyond the protected area perimeter must be installed in conduit and must employ electronic line supervision. Electronic line supervision will entail a polling or multiplexing system or equivalent. If line supervision is unavailable, two independent means of alarm signal transmission to the monitoring location must be provided.
- All system sensors must be located within the protected area.
- Cabling between all sensors and the PCU must be dedicated to the system, contained within the protected area.

C-3.4 Emergency Backup Electrical Power.

- Eight hours of uninterruptible backup power is required³. This may be provided by an uninterruptible power supply (UPS), batteries integral to the ESS, generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.
- An audible or visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the monitoring station must visibly and audibly indicate a failure in a power source or a change in power source.

C-4 MAGAZINE



C-4.1 Policy Baseline.

- DoD Manual 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E),
- OPNAV INSTRUCTION 5530.13C Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives.
- MCO 5530.14A Marine Corps Physical Security Program Manual
- AFI 31-101 Department of the Air Force Integrated Defense
- AR 190-11 Department of the Army Physical Security of Arms, Ammunition, and Explosives

C-4.2 Baseline Intrusion Detection System (IDS) Requirements.

³ Based on DoD O-2000.12-H, Antiterrorism Handbook

- Must be protected by an IDS when not continuously manned or under constant surveillance.
- All perimeter doors and man-passable openings into the magazine must be protected by High Security Switch (HSS) and a motion detection sensor.
- Keypad at entrance of all separated (unit-based) storage areas that require an independent IDS capability.
- IDS must be installed in accordance with UL 681 and consist of:
 - Level 2 high security switches (HSS) that meet UL 634, and/or other government approved sensors.
 - Motion detection sensors UL 639 listed.
- Premise Control Units (PCUs) should be located within the protected area.

C-4.3 Tamper Protection.

- All IDS systems, including any access control system connected must be equipped with tamper detection devices that must be monitored continuously whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU or monitoring station.
- System associated cabling that extends beyond the protected area perimeter must be installed in conduit and must employ electronic line supervision. Electronic line supervision will entail a polling or multiplexing system or equivalent. If line supervision is unavailable, two independent means of alarm signal transmission to the monitoring location must be provided.
- All system sensors must be located within the protected area.
- Cabling between all sensors and the PCU must be dedicated to the system, contained within the magazine.

C-4.4 Emergency Backup Electrical Power.

- Eight hours of uninterruptible backup power is required⁴. This may be provided by an uninterruptible power supply (UPS), batteries integral to the ESS, generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.
- An audible or visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the

⁴ Based on DoD O-2000.12-H, Antiterrorism Handbook

monitoring station must visibly and audibly indicate a failure in a power source or a change in power source.