

UNIFIED FACILITIES CRITERIA (UFC)

SECURITY ENGINEERING ELECTRONIC SECURITY SYSTEMS



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

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 SUPPORT AGENCY

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

Change No.	Date	Location
1	23 Oct 06	Title adjusted

FOREWORD

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

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

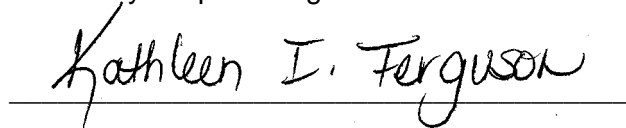
•

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

AUTHORIZED BY:



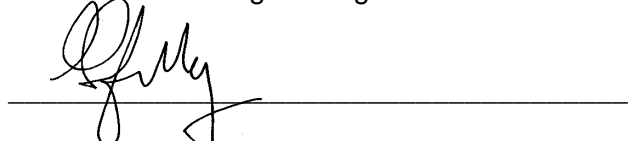
DONALD L. BASHAM, P.E.
Chief, Engineering and Construction
U.S. Army Corps of Engineers



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



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



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

Unified Facilities Criteria (UFC)

New Document Summary Sheet

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

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

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

Reasons for Development:

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

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

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

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

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

CONTENTS

CHAPTER 1 INTRODUCTION.....	8
1-1 PURPOSE	8
1-2 SCOPE	8
1-3 REFERENCES	8
1-4 GLOSSARY	9
1-5 SECURITY ENGINEERING UFC SERIES	9
1-6 ORGANIZATION OF THIS UFC	10
CHAPTER 2 ELECTRONIC SECURITY SYSTEM OVERVIEW	12
2-1 OVERVIEW.....	12
2-2 DETECT, DELAY, AND RESPOND.....	12
2-3 ESTABLISH REQUIREMENTS	16
2-4 SYSTEM COMPLEXITY	18
2-5 MONITORING METHODS.....	20
CHAPTER 3 ACCESS CONTROL SYSTEMS.....	24
3-1 OVERVIEW.....	24
3-2 ACS ENTRY-AUTHORIZATION IDENTIFIERS.....	26
3-3 OTHER ACS IMPLEMENTATION CONSIDERATIONS	28
3-4 ACS EQUIPMENT	31
3-5 ACS DESIGN GUIDANCE	41
CHAPTER 4 CLOSED CIRCUIT TELEVISION SYSTEMS.....	44
4-1 OVERVIEW.....	44
4-2 DIGITAL VIDEO RECORDER (DVR).....	46
4-3 SYSTEM DISPLAYS.....	46
4-4 VIDEO MATRIX SWITCHERS.....	53
4-5 KEYBOARDS.....	53
4-6 CAMERAS	53
4-7 INTERNET PROTOCOL (IP) ADDRESSABLE CAMERAS	57
4-8 RECORDING	58
4-9 ILLUMINATION.....	59
4-10 VIEWING IN LOW-LIGHT CONDITIONS.....	61
4-11 POWER	62
4-12 CAMERA FIELDS-OF-VIEW.....	62
4-13 RESOLUTION.....	64
4-14 FRAMES PER SECOND (FPS)	65
4-15 BANDWIDTH	65
4-16 WHITE BALANCE.....	67
4-17 CCTV CAMERA EMPLOYMENT FOR INTRUSION DETECTION	67
4-18 CCTV EQUIPMENT CONSIDERATIONS.....	69
4-19 CCTV SYSTEMS DESIGN GUIDANCE.....	71

CHAPTER 5	INTRUSION DETECTION SYSTEM	75
5-1	OVERVIEW.....	75
5-2	CENTRAL PROCESSING UNIT (CPU)	75
5-3	INTERIOR SENSORS	75
5-4	EXTERIOR SENSORS	82
5-5	SYSTEM CONFIGURATION	93
5-6	IDS DESIGN GUIDANCE	93
5-7	SUMMARY	96
CHAPTER 6	DATA TRANSMISSION MEDIA (DTM)	97
6-1	INTRODUCTION	97
6-2	BANDWIDTH ANALYSIS.....	97
6-3	SECURE COMMUNICATIONS.....	98
6-4	NETWORK TOPOGRAPHY	98
6-5	COMMUNICATION REDUNDANCY.....	103
6-6	TRANSMISSION MODES/PROTOCOLS	103
6-7	TRANSMISSION MEDIA	103
6-8	TECHNOLOGY COMPARISION	105
6-9	ENCRYPTION	105
CHAPTER 7	DISPATCH CENTER	107
7-1	INTRODUCTION	107
7-2	SPACE.....	108
7-3	LIGHTING.....	109
7-4	CONSOLES	109
7-5	MONITORS.....	111
7-6	GROUNDING/POWER CONDITIONING.....	111
7-7	HVAC.....	111
7-8	SUPPORT ROOMS	112
CHAPTER 8	ESS SUBSYSTEM INTEGRATION	113
8-1	OVERVIEW.....	113
8-2	COMMUNICATION FROM THE IDS TO THE ACS.....	113
8-3	COMMUNICATION FROM THE IDS TO THE CCTV SYSTEM.....	113
8-4	COMMUNICATION FROM THE CCTV SYSTEM TO THE ACS	114
8-5	COMMUNICATION FROM THE ACS TO THE DISPATCH CENTER	115
8-6	COMMUNICATION FROM THE DISPATCH CENTER TO THE ACS	115
8-7	BANDWIDTH ANALYSIS.....	115
CHAPTER 9	GENERAL REQUIREMENTS AND CROSS-DISCIPLINE COORDINATION	117
9-1	GENERAL REQUIREMENTS	117
9-2	GENERAL COORDINATION	118
9-3	CIVIL COORDINATION	118
9-4	ARCHITECTURAL COORDINATION	118
9-5	LIFE SAFETY CODE CONSIDERATIONS.....	121

9-6 ELECTRICAL COORDINATION 121
9-7 MATERIAL ENTRY CONTROL 129

CHAPTER 10 MODEL DESIGN APPROACH..... 130
10-1 INTRODUCTION 130
10-2 PROJECT PLANNING 130
10-3 INITIAL DRAWING PREPARATION 131
10-4 BASIS OF DESIGN 131
10-5 SCHEMATIC DESIGN PHASE 134
10-6 DESIGN DEVELOPMENT PHASE 134
10-7 BIDDING 134

APPENDIX A REFERENCES 135

APPENDIX B GLOSSARY 138
ACRONYMS AND ABBREVIATIONS..... 138
DEFINITION OF TERMS..... 141

Table of Figures and Tables

Figure 2-1. ESS as a Part of a Physical Security System	13
Figure 2-2. Example Detect and Delay Options	14
Table 2-1. Example Breach Events and Delay Time	14
Table 2-2. Sample Detect, Delay, and Respond Measures.....	14
Figure 2-3. Timeline Showing Two Cases of Breach and Detection	15
Figure 2-4. Project Process.....	17
Figure 2-5. A Simple ESS System	18
Figure 2-6. Intermediate System with Separate ACS and IDS.....	18
Figure 2-7. Complex System With Separate ACS, IDS, and CCTV Subsystems.....	19
Figure 2-8. Networked System.....	20
Figure 2-9. Local Alarm Monitoring	21
Figure 2-10. Central Station Monitoring.....	21
Figure 2-11. Police Connection Monitoring	22
Figure 2-12. Proprietary Station Monitoring.....	22
Table 2-3 Pros and Cons of Monitoring Methods	22
Figure 3-1. Example Access Control System (ACS)	25
Figure 3-2. Advantages and Disadvantages of Using Credential Devices	26
Figure 3-3. Advantages and Disadvantages of Using Coded Devices	27
Figure 3-4. Advantages and Disadvantages of Using Biometric Devices.....	28
Table 3-1 Exit Technologies (Pros and Cons).....	30
Figure 3-5. Basic Access Control Sequence.....	33
Figure 3-6. PCU In A SCIF.....	34
Figure 3-7. Sample Card Reader Door Configuration	36
Figure 3-8. ACS Design Process	43

Figure 4-1. Example CCTV System	45
Figure 4-2. Dimensions of a “9-inch” ESS Display	47
Figure 4-3. Example of a “Quad-Screen” Display	49
Figure 4-4. “Switching” Two Camera Images on a Single Display	50
Table 4-1. CCTV-Display Component Application Guidance	51
Figure 4-5. Simple Two Display Monitor Configuration	52
Figure 4-6. Multiple Images on A Single Display	52
Figure 4-7. Pre-alarm, Current, and Post-Alarm Image Comparison	52
Figure 4-8. PTZ Sweep Range.....	56
Table 4-2. Fixed versus PTZ Cameras.....	56
Figure 4-9. Calculation for Storage of Frame Size of 25 kbytes	58
Table 4-3. Light-to-Dark Ratios	60
Table 4-4. Characteristics of Thermal Imagers	62
Figure 4-10. Relative Magnification of an Object.....	63
Figure 4-11. Field-of-view and Focal Length	64
Figure 4-12. Calculation For a Camera in Nonalarm Mode at 2 FPS	65
Figure 4-13. Calculation For a Camera in Alarm Mode at 10 fps	66
Table 4-5. CCTV Design Guidance and Recommendations	72
Figure 5-1. Example Intrusion Detection System (IDS).....	76
Figure 5-2. Separate ACS and IDS CPUs.....	77
Figure 5-3. Sample Door Configuration.....	78
Figure 5-4. Sample Window Configuration.....	78
Figure 5-5. Sample Roof Hatch Configuration.....	79
Table 5-1. Application Notes – Interior IDS Sensors	82
Figure 5-6. Active Infrared IDS.....	83

Figure 5-7. Monostatic Microwave Sensor and Associated Footprints 84

Figure 5-8. Bistatic Microwave Sensor Operation 85

Figure 5-9. Typical Bistatic Microwave Layout and Guidance 86

Figure 5-10 Video Intrusion Detection System 87

Table 5-2. Video IDS Design Guidance and Recommendations 88

Figure 5-11. Typical Fiber Optic Fence Detection System 90

Figure 5-12. Fence Example 91

Table 5-3. False Alarm Causes—Exterior IDS Sensors 92

Table 5-4. Advantages and Disadvantages of “AND” and “OR” Configurations 93

Table 5-5. Sample Probability of Detection Factors 93

Figure 5-13. Zoned Detection System..... 94

Table 5-6. IDS Design Guidance..... 95

Table 5-7 Exterior IDS Applications Table..... 96

Table 6-1. Example Bandwidth Calculations 98

Figure 6-1 Star Topographies 100

Figure 6-2. Ring Topographies..... 101

Figure 6-3. Fully-Meshed Topographies..... 102

Figure 6-4. Single-Mode Fiber Optic 104

Figure 6-5. Multi-Mode Fiber Optic..... 104

Table 6-2. DTM Technologies for ESS..... 106

Figure 7-1. Dispatch Center Centrally Located 107

Figure 7-2. Example RDC 108

Figure 7-3. Sample Simple Dispatch Center Console Layout 110

Figure 7-4. Sample Small-Medium Dispatch Center Space Layout 110

Figure 8-1. Sample DTM System Detail 115

Table 9-1. Voltage Drop 125

Figure 9-1. Attempts 1 and 2..... 126

Figure 9-2. Interface Between Fire alarm and Security Panel 127

Figure 10-1 Cable Counts on Riser Diagrams..... 132

Figure 10-2. Sample Cable Schedule..... 132

Figure 10-3. Functional Matrix..... 133

CHAPTER 1

INTRODUCTION

1-1 PURPOSE

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

1-2.1 Applicability

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

1-2 SCOPE

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

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

1-3 REFERENCES

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

1-4 GLOSSARY

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

1-5 SECURITY ENGINEERING UFC SERIES

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

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

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

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

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

1-5.4 **Security Engineering Facilities Design Manual.** UFC 4-020-02 (not published at the time of this printing) provides interdisciplinary design guidance for developing preliminary protective measures systems to implement the design criteria

established using UFC 4-020-01. Those protective measures include building and site elements, equipment, and the supporting manpower and procedures necessary to make them all work as a system. The information in UFC 4-020-02 is in sufficient detail to support concept-level project development and provides a sound basis for a more detailed design. This UFC also provides a process for assessing the impact of protective measures on risk. The primary audience for the "Security Engineering Facilities Design Manual" is the design team, which should include security (Physical Security Officer) and antiterrorism personnel. Security is an essential part of the design team and they should bring in antiterrorism personnel (Antiterrorism Officer ATO), when appropriate.

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

1-6 ORGANIZATION OF THIS UFC

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

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

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

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

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

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

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

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

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

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

CHAPTER 2

ELECTRONIC SECURITY SYSTEM OVERVIEW

2-1 OVERVIEW

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

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

2-2 DETECT, DELAY, AND RESPOND

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

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

2-2.3 Conversely, assuming a security forces response time of five minutes, the sequence of events shown in Table 2-1 allows sufficient time to intervene on the

intrusion efforts. In designing an ESS, the designer should work with the facility/base security officer to identify the response forces and reaction times.

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

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

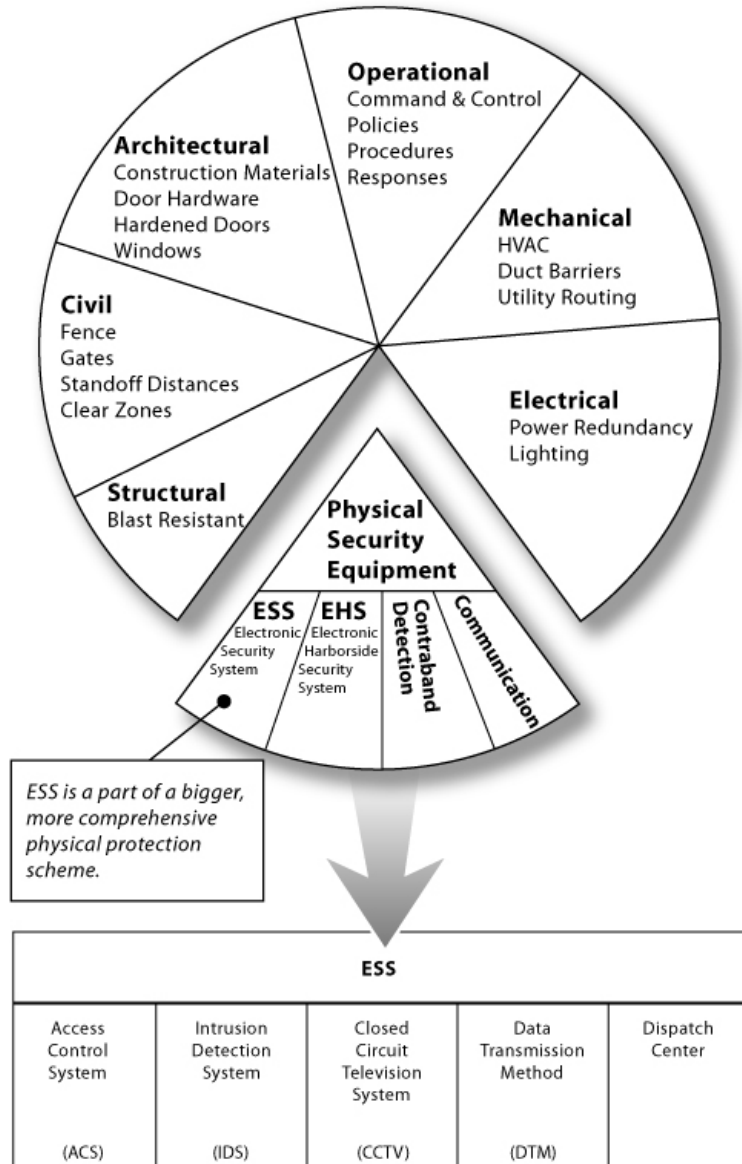


Figure 2-2. Example Detect and Delay Options

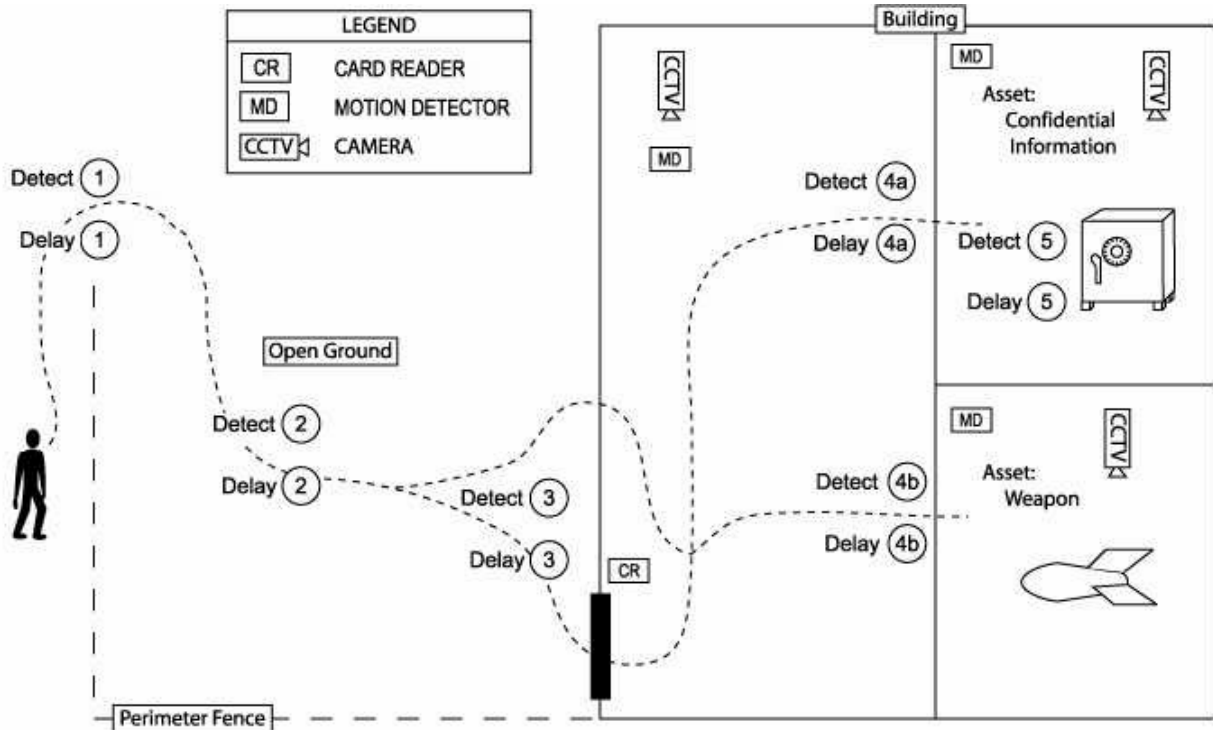


Table 2-1. Example Breach Events and Delay Time

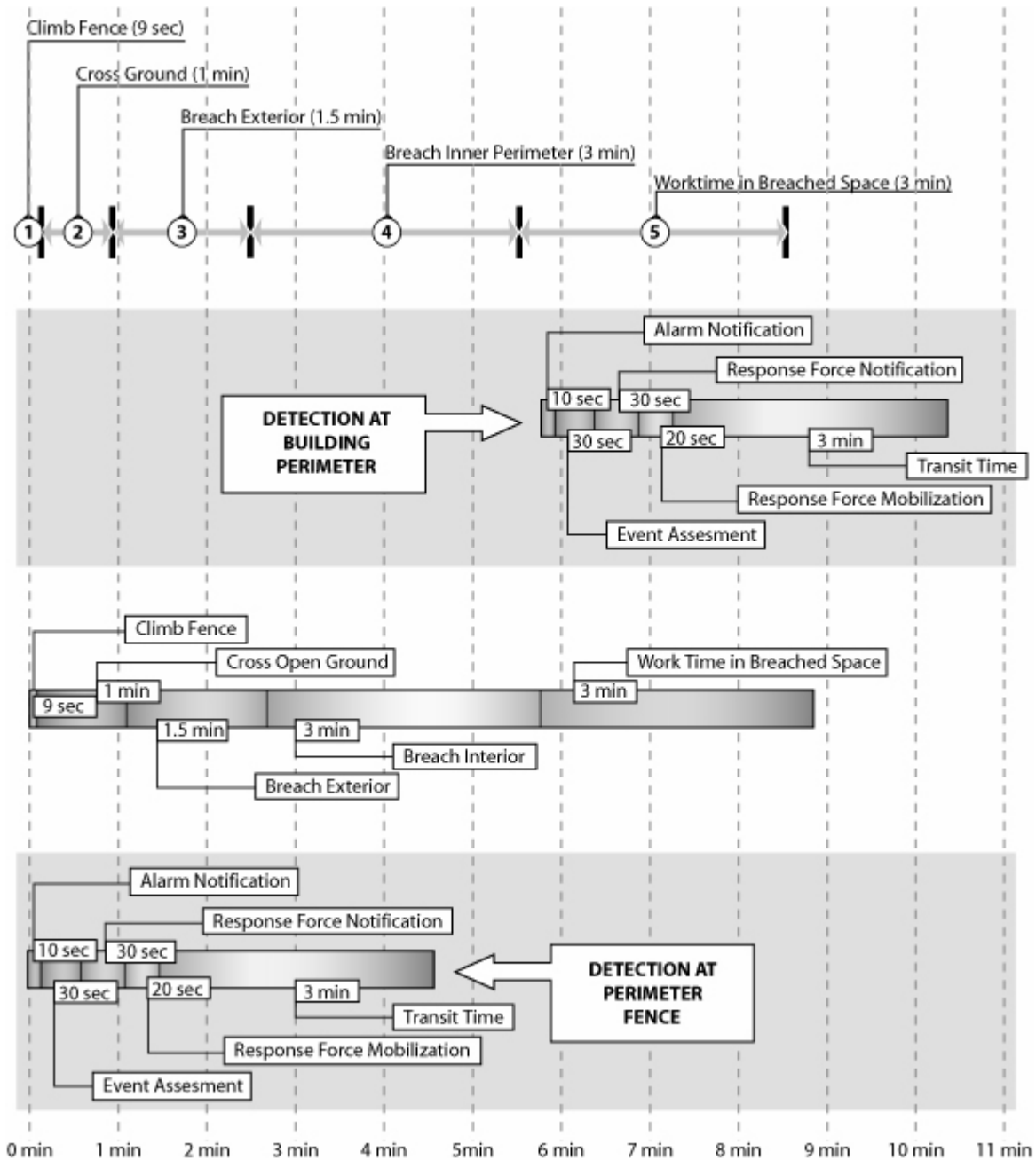
	Delay Options	Delay Time	Detection Options
1	Climb fence	8-10 sec.	Perimeter fence detection system
2	Cross open ground	10 feet/sec.	Microwave sensors
3	Breach building door or window or wall	1-2 min.	Door contacts or glass breakage sensor
4	Breach interior hardened door	2-4 min.	Door contacts
5	Work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

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

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

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

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



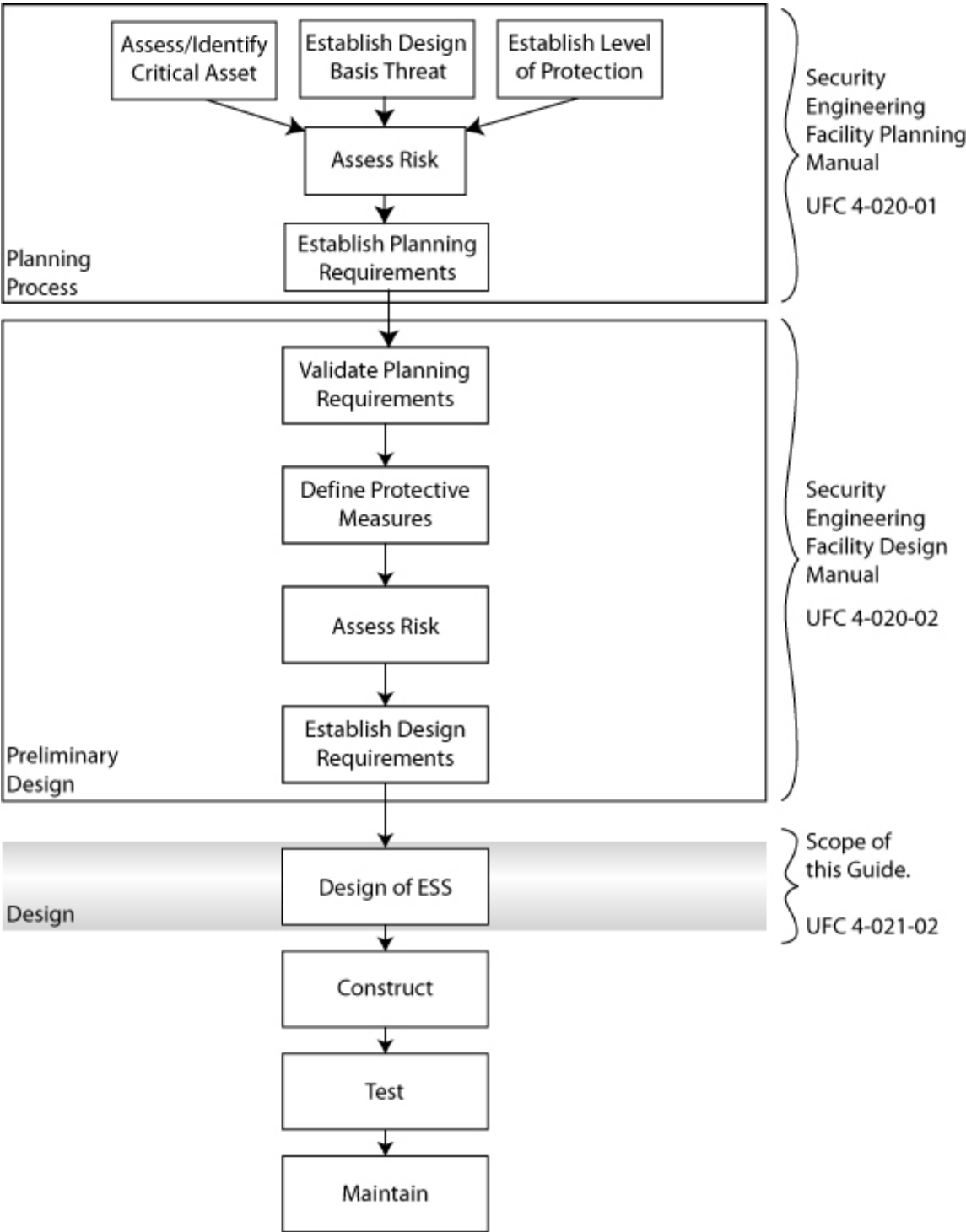
In the above timeline, there will be a difference in time required to provide protection depending on whether or the desired protection is to prevent compromise or prevent destruction. If the goal is to prevent compromise of the asset, the response force must arrive in time to prevent the threat from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

2-3 ESTABLISH REQUIREMENTS

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

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

Figure 2-4. Project Process



2-4 SYSTEM COMPLEXITY

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

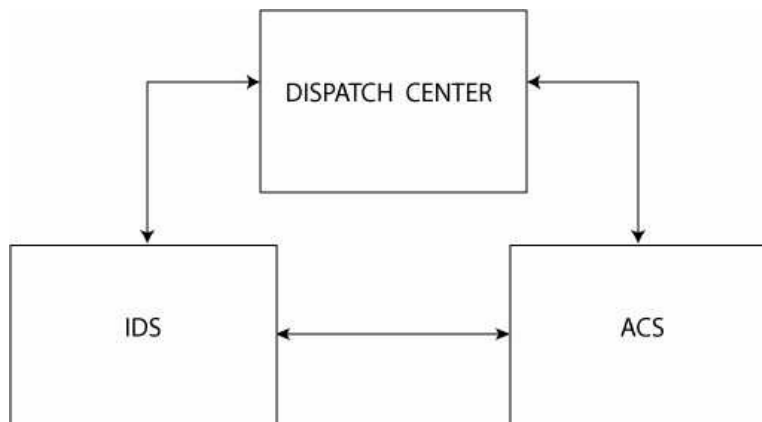
2-4.2 **Simple System.** The simplest ESS consists of a single ESS subsystem. For example, a simple IDS at a low value asset is a simple system as shown in Figure 2-5. Other examples are an IDS with door contact, motion sensors, break-glass sensors and other digital input type sensors that do not require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

Figure 2-5. A Simple ESS System



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

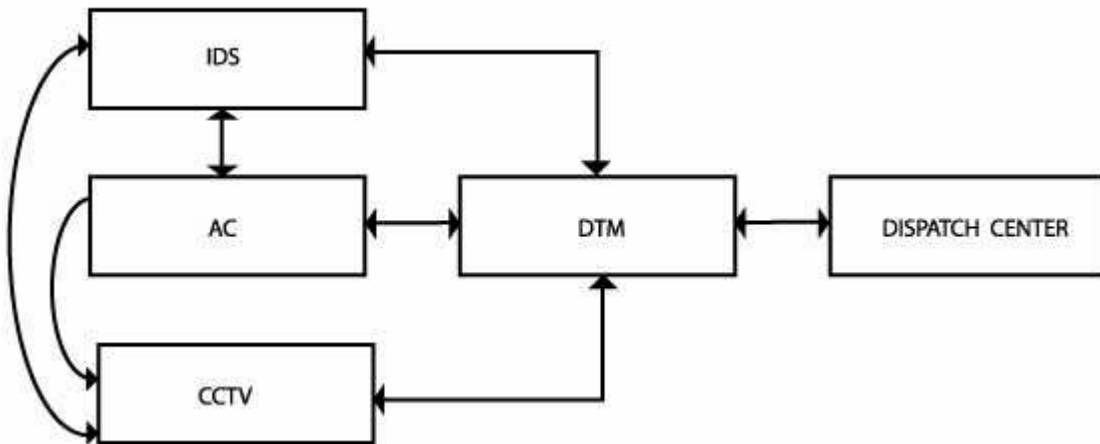
Figure 2-6. Intermediate System with Separate ACS and IDS



2-4.3.1 **Combining ACS and IDS.** Virtually all ACS can accommodate digital input signals. Quite often it is possible to combine ACS and IDS when the IDS inputs are limited to simple digital input devices that do not require separate IDS controllers. Examples of these types of digital input IDS devices are door contacts, glass-break sensors, and motion sensors.

2-4.4 **Complex System.** A complex system has a separate ACS and IDS system as well as a CCTV system communicating to a Dispatch Center through a DTM as shown in Figure 2-7.

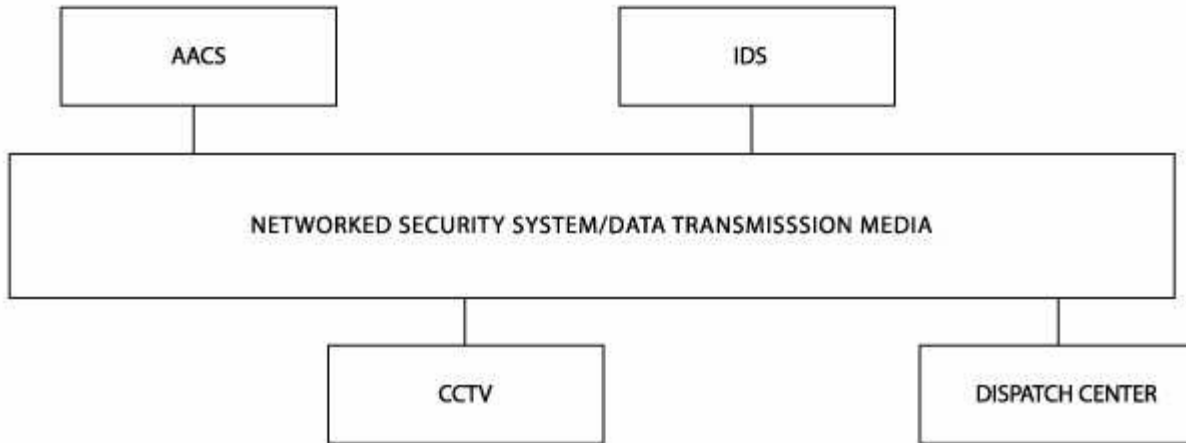
Figure 2-7. Complex System With Separate ACS, IDS, and CCTV Subsystems



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

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

Figure 2-8. Networked System



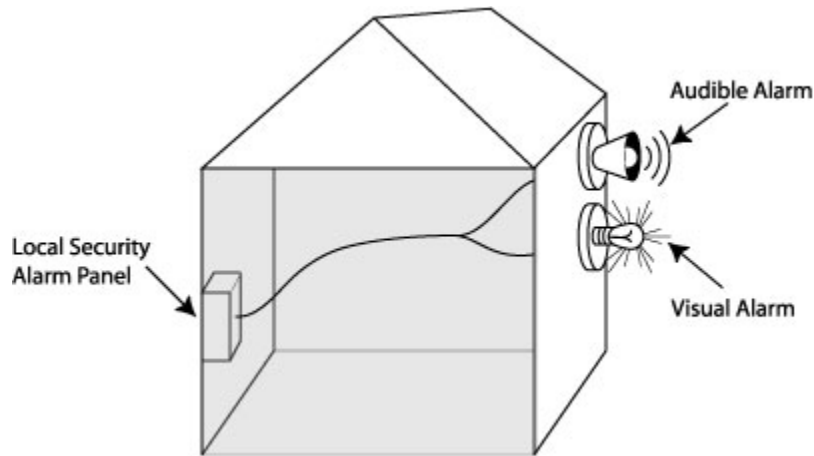
The networked security system operates on a single network with drivers to the different discrete components of the subsystems. While it is possible to procure networked systems, security suppliers are at different stages of development of providing networked systems for all ESS capabilities. At this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

2-5 MONITORING METHODS

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

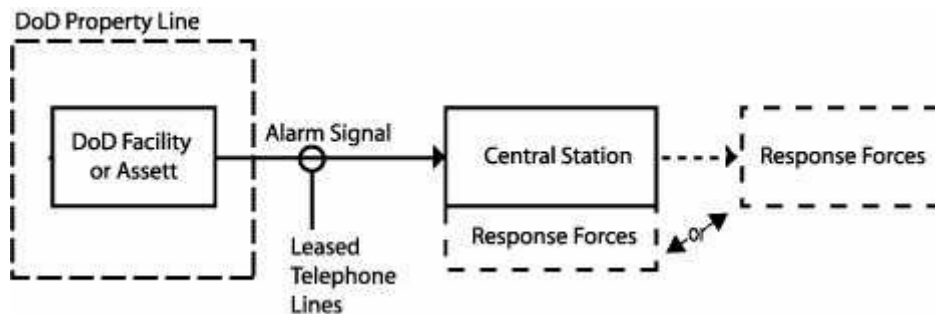
2-5.2 **Local Alarm.** Local alarms actuate a visible and/or audible signal, usually located on the exterior of the facility. Refer to Figure 2-9. Alarm transmission lines do not leave the facility. Response is generated from security forces located in the immediate area. Without security forces in the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

Figure 2-9. Local Alarm Monitoring



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

Figure 2-10. Central Station Monitoring



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

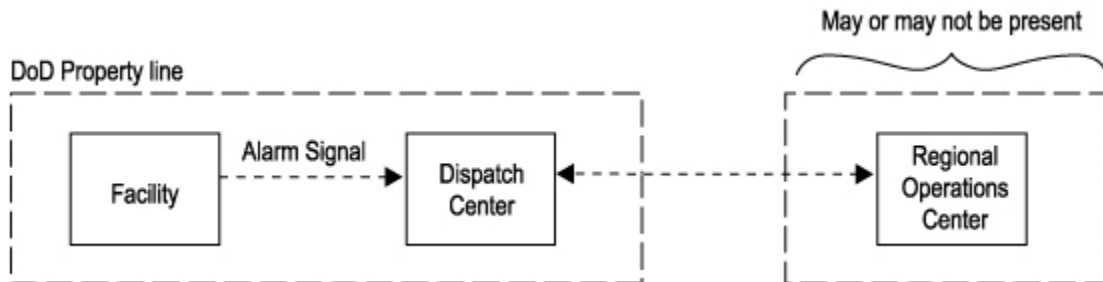
connection configuration, include medical clinics, base exchanges, commissaries, and Reserve Centers. Refer to Figure 2-11 for a diagram of a police station connection.

Figure 2-11. Police Connection Monitoring



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

Figure 2-12. Proprietary Station Monitoring



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

Table 2-3 Pros and Cons of Monitoring Methods

	Pros	Cons
Local Alarm Station	<ul style="list-style-type: none"> Easy to implement Cost effective Simple 	<ul style="list-style-type: none"> No guaranteed response, relies on support forces being in audible/visual range
Centralized Station	<ul style="list-style-type: none"> Does not require any additional space or building Probably does not require any additional staffing 	<ul style="list-style-type: none"> Requires an existing Central Station Some complexity in establishing connection May rely on non-DoD forces CCTV capability may be limited or non-existent

<p>Police Connection</p>	<p>Direct communication with law enforcement/response forces without delay.</p>	<p>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.</p>
<p>Proprietary Station</p>	<p>Not reliant on outside sources. Should have CCTV assessment capability. May have Motion Path Analysis (IDS) capability.</p>	<p>Requires 24/7 trained personnel; possibly increased staffing. Requires real estate space and fit-out hardware. Increased recurring labor cost of Dispatch Center operators.</p>