Student Guide

Electronic Security Systems

Course Overview

Course Introduction

Course Overview

Every day, on our military installations and DoD facilities, we protect a wide variety of assets from various types of threats.

One way we do this is through surveillance—that is, by using electronic sensors, cameras, and automated access control systems as well as security forces to monitor those systems. In this course, you will learn about some different types of electronic security systems. You will also learn how each is used as a stand-alone measure and how you can use them together to better protect valuable assets. Welcome to the Electronic Security Systems course.

Course Objectives

Here are the course objectives.

- Define the purpose of electronic security systems (ESS)
- Identify the purpose and roles of the subsystems that compose ESS
- Identify applicable references and policies for specific types of and best uses for ESS
- Apply the baseline requirements for ESS for Sensitive Compartmented Information Facilities (SCIFs), Top Secret/Secret open storage areas, conventional arms storage areas/armories, and magazines
- Identify key planning considerations for ESS implementation

Student Guide

Electronic Security Systems

Lesson 1: ESS Overview

Introduction

Objectives

In this lesson, you will learn what electronic security systems (ESS) are and the subsystems that compose them. You will also learn about key planning considerations for implementing ESS. Here are the lesson objectives:

- Define the purpose of electronic security systems (ESS)
- Identify applicable references and policies for specific types of and best uses for ESS
- Identify key planning considerations for ESS implementation

What is an ESS?

Overview

We use a variety of physical security measures to protect our personnel, information, equipment, facilities, activities, and operations. Combining these elements creates an overall physical protection system that includes measures such as:

- Blast-resistant materials on our buildings
- Hardened doors and protected windows
- Fences, gates, and clear zones around our perimeters
- Barriers on our ducts and other man-passable openings
- Security lighting in and around our facilities
- Numerous physical security policies and procedures

Of course no physical protection system would be complete without physical security equipment, which includes ESS. An ESS is an integrated electronic system that is part of an overall physical protection system.

An ESS may include one or more of these subsystems:

- Automated access control systems (AACS)

- Interior and exterior intrusion detection systems (IDS)
- Closed circuit television (CCTV) systems
- Data transmission media (DTM)
- Monitoring centers

Later in this course, you'll learn more about the purpose and role of each of these subsystems.

Detect, Delay, Respond Principle

In order to be effective, an ESS should be able to detect an intrusion and allow for a quick response to it, to prevent any potential compromise. This is referred to as the Detect, Delay, Respond Principle.

Let's look at how this works. Imagine someone attempts to break into your facility. Once your system detects the intrusion, the clock starts running. Your security forces need to respond as quickly as possible to prevent any damage to or compromise of your facility's assets.

Once your ESS detects an intrusion, it is very important for the system to also have the capability to assess what triggered it. For example, having a CCTV camera feed overlooking a gate protected by a sensor will give you additional information about what happened to set off an alarm. This assessment capability will assist you in determining the most appropriate security response.

Planning Considerations

Considerations Overview

When planning how to protect assets with an ESS, you must consider several different factors. You need to assess and manage the risks to your assets. You need to identify and comply with applicable regulatory requirements. You need to consider the characteristics of the site you are protecting, as well as its operational requirements. And finally, you need to take into account cost considerations and constraints.

Let's take a look at each of these planning considerations.

Risk Management

As with any other type of physical security measure, following a risk management process will help you determine which ESS, if any, will best protect your facility's assets.

This risk management process has five steps: identify assets, threats, and vulnerabilities, then conduct a risk analysis and develop countermeasures to address certain risks. Let's take a look at each step to see how it applies to ESS.

Identify Assets

The first step of the risk management process is to identify assets. You must work with the end-user to identify anything that requires protection. Examples of assets include people, information, equipment, facilities, activities, and operations. Once you have identified the assets, you should group them into categories of assets requiring similar protection. Then you should determine the level of protection each category requires.

Identify Threats

The second step of the risk management process is to identify threats. Threats come in many forms such as terrorists, extremists, criminals, insiders, and spies. Once you know the potential threats to your assets, you must consider what types of actions they can inflict. Some examples include theft, attacks, disruption of services, sabotage, kidnapping, and death. For military facilities, threats should already be identified and documented in a threat assessment.

Identify Vulnerabilities

The third step of the risk management process is to identify vulnerabilities or weaknesses. Vulnerabilities are anything that can be exploited by a threat. Another way to look at vulnerabilities is as the difference between the protection that exists and the protection that is needed to protect an asset from a threat. You can use the results of your threat assessment to help determine your vulnerabilities.

Conduct Risk Analysis

The fourth step of the risk management process is to conduct a risk analysis. In a risk analysis, you must determine the consequences or impact of a threat event and the likelihood of the threat occurring. There are situations where some level of risk is acceptable; for example, if the impact of the threat is low or the probability of occurrence is low. Once you complete your analysis, you can move to the next step of the process and develop countermeasures for the greatest risks.

Develop Countermeasures

The final step of the risk management process is to determine and develop which countermeasures will best protect your assets against the threats you identified. Countermeasures aim to prevent adverse occurrences or reduce the impact of them, if they happen. An ESS is a countermeasure. Electronic security systems are used to detect, assess, delay, and respond to intrusions, which helps to prevent or at least reduce the impact of adverse occurrences.

Regulatory Requirements

When planning for the use of ESS, you must follow regulatory guidance. Many ESS requirements are established by applicable regulations.

The primary guidance documents for ESS are Unified Facilities Criteria (UFC) 4-021-02, Electronic Security Systems and Underwriters Laboratory (UL) 639, Standard for Intrusion Detection.

In addition, regulatory guidance has been developed for special areas that require additional protection. This includes:

- ICS 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities
- DoDM 5105.21, Vol. 1-3, Sensitive Compartmented Information Administrative Security Manual
- DoDM 5200.01, Vol. 3, DoD Information Security Program
- DoDM 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives.

Refer to your Component for Component-specific guidance related to ESS.

Site Survey

An important step in planning for ESS is to conduct a site survey. The site survey team should include personnel from a variety of areas of expertise, such as an electronic security professional, a physical security professional, a communications/ information technology professional, an electrical engineer, a mechanical engineer, a civil/structural engineer, a life safety engineer, and an architect.

During the site survey, obtain the site plan and/or building plans and conduct a capacity assessment to see if any ESS already exist. Interview key personnel at the site such as users, operational level personnel, and middle management to gain perspective and information about the protection of assets at that site. Then assess any existing systems and note any vulnerabilities in how they protect key assets. After the site survey, review the threat summary, recommend ways to correct the vulnerabilities you identified, and propose new countermeasures, such as ESS and its locations, to protect assets, if necessary.

Operational Requirements

In planning an ESS, you must consider operational requirements, such as the facility requirements and security force requirements. For example, some ESS require security personnel to monitor automated access control systems, either in person or via a camera. Others require security personnel to assess alarms, and in some cases, respond to the scene of an intrusion.

Cost Considerations, Constraints, and Tools

As with any project, cost is a major consideration when determining ESS requirements. You must balance the value of the asset, which could be a monetary value, human life, or the asset's criticality in protecting national security, depending on what type of asset it is, with the cost of protecting that asset. In addition to the actual cost of an ESS, you must factor in the cost to operate and maintain that system. You must also balance project funding with project scope. And you need to consider other factors, such as life safety and convenience. There are tools available, such as the Army Corps of Engineers Cost Estimator, which can assist in determining the cost of a project.

Review Activity

Review Activity 1

Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	True	False
An ESS is a component of an overall physical protection system.	○	○
An ESS must be comprised of at least two or more subsystems. Therefore, a stand-alone automated access control system, for example, would not constitute an ESS.	○	○
An effective ESS must ensure that 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.	○	○

Review Activity 2

You are tasked with planning an ESS for a DoD facility. What regulatory guidance document(s) should be your primary reference?

Select the best answer. Check your answer in the Answer Key at the end of this Student Guide.

- o DoDM 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- o UFC, 4-021-02, Electronic Security Systems
- o ICS 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities
- o DoD Manual on ESS Planning

Review Activity 3

Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	True	False
Assets, threats, and vulnerabilities are all part of the risk calculation.	○	○
Threats against an asset are determined when you conduct a site survey.	○	○
You must consider operational and maintenance costs of an ESS when comparing the value of an asset to be protected versus the cost of the ESS to protect an asset.	○	○

Answer Key - Review Activities

Review Activity 1

Select True or False for each statement.

	True	False
An ESS is a component of an overall physical protection system.	⊙	○
Feedback: *An ESS is a component of the physical security equipment component of an overall physical protection system.*		
An ESS must be comprised of at least two or more subsystems. Therefore, a stand-alone automated access control system, for example, would not constitute an ESS.	○	⊙
Feedback: *An ESS is comprised of one or more subsystems. Therefore, a stand-alone automated access control system would constitute an ESS.*		
An effective ESS must ensure that 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.	⊙	○
Feedback: *An effective ESS should operate on the Detect, Delay, Respond principle, which ensures that 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.*		

Review Activity 2

You are tasked with planning an ESS for a DoD facility. What regulatory guidance document(s) should be your primary reference?

Select the best answer.

- ○ DoDM 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- ◉ UFC, 4-021-02, Electronic Security Systems
- ○ ICS 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities
- ○ DoD Manual on ESS Planning

Feedback*: The primary guidance for ESS is UFC, 4-021-02, Electronic Security Systems. You can find additional guidance in regulations governing specific types of areas, as well as in Component-specific guidance.*

Review Activity 3

Select True or False for each statement.

	True	False
Assets, threats, and vulnerabilities are all part of the risk calculation.	⊙	○
Feedback: *Assets, threats, and vulnerabilities are all part of the risk calculation. Countermeasures are determined and developed to reduce risk.*		
Threats against an asset are determined when you conduct a site survey.	○	⊙
Feedback: *Threats against an asset are determined through a threat assessment. Vulnerabilities can be determined during a site survey.*		
You must consider operational and maintenance costs of an ESS when comparing the value of an asset to be protected versus the cost of the ESS to protect an asset.	⊙	○
Feedback: *Operational and maintenance costs of an ESS must also be considered when comparing the value of an asset to be protected versus the cost of the ESS to protect an asset.*		

Student Guide

Electronic Security Systems

Lesson 2: Automated Access Control Systems

Introduction

Objectives

In this lesson, you will learn what automated access control systems (AACS) are and the planning considerations for implementing an AACS. You will also learn about the different types of AACS and the components of AACS.

Here are the lesson objectives:

- Identify the purpose and role of automated access control systems
- Identify key planning considerations for AACS implementation

What Are Automated Access Control Systems?

Overview

An AACS is an automated system that interfaces with locking mechanisms to momentarily permit access to a controlled area. It does this by unlocking doors, gates, or turnstiles after verifying entry credentials, such as a user's identification card. An AACS ensures that only authorized personnel can access a controlled area, which helps prevent unauthorized persons from entering it.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

> ***Physical Access Control Systems (PACS)***
>
> Access control systems must meet the security objectives of Homeland Security Presidential Directive 12 (HSPD12), including personal identity proofing, registration, and issuance. The Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors describes the minimum requirements and provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. **For more information, please**

visit the Identity Credential Access Management (ICAM) web site at www.idmanagement.gov.

Where electronic physical access control systems are not appropriate due to limited access control or mission requirements, a physical and visual inspection of cards as authorized by internal policy shall be conducted by security forces and/or guards at physical entry and/or access control points. This inspection includes:

- Visual match of the photograph on the card to the person presenting the identification
- Comparison and visual review of the card for unique topology and security design requirements
- Verification of authenticity by checking the anti-counterfeit and/or fraud protection measures embedded in the credential

When funding becomes available, installations will procure an electronic PACS that provides the capability to rapidly and electronically authenticate credentials and individuals authorization to enter an installation. The PACS must:

- Support a DoD-wide and federally interoperable access control capability that can authenticate US government physical access credentials and support access enrollment, authorization processes, and securely share information
- Interface with locking mechanism
- Permit access to a controlled area after verifying credentials
- Delay/deny intruders

Capabilities of AACS

An AACS has many capabilities that can be employed depending on the types of security requirements. An AACS can log and archive all entry attempts and entries made into a controlled area and can alert authorities of unauthorized entry attempts. An AACS can alert authorities by interfacing with other electronic security system (ESS) subsystems. For example, an AACS can interface with a closed circuit television (CCTV) system to assist security personnel in assessing unauthorized entry attempts or to verify the identity of entrants before manually granting access, such as through a remote door or gate. An AACS can also interface with an intrusion detection system (IDS) to sound an alarm if someone makes an unauthorized entry or entry attempt. In addition, an AACS can transmit signals to a dispatch or control center so security personnel may respond to an unauthorized entry attempt, if necessary.

Planning Considerations

Planning Overview

When planning for an AACS, there are many factors to consider. These include who will be using the system, what the security and tracking requirements are for the portal requiring access control, what the facility and security force operational requirements are, and life safety considerations. Let's take a look at each of these planning considerations.

Users

For each AACS, you must determine who will be using the system. How many credential holders and what categories of personnel will use this AACS? How many visitors and contractors will pass through this system? This is important because you want to implement the most cost-effective system that allows authorized personnel to quickly enter a protected area while also denying entrance to unauthorized personnel.

Security Requirements

To ensure your AACS is secure, you must consider various security-related questions.

- How many levels of credentials or tokens are required?

  For example, if the requirement is simple, then access with a common access card (CAC) alone may suffice. If you need increased security, then you may want to require a personal identification number (PIN) in conjunction with a CAC. If the requirement is for maximum security, then the AACS may need to require a CAC, a PIN, and biometrics (such as a fingerprint or retina scan) to allow access.

- How many and what types of portals will you need to protect? And what locking method will secure those portals?

- How long can the system take to identify, verify, and authenticate the information of a person as authorized to enter a controlled area?

  This is known as a throughput requirement. Combining credentials results in increased verification time and will decrease throughput rate—fewer people will be able to gain access in a fixed amount of time.

- Does the system need to eliminate or mitigate the risk of someone giving their credentials to another person to access the controlled area?

  If so, then the AACS will require the anti-passback feature.

- Does your system need to protect against a person following another closely in order to enter through the same portal when the authorized person's credential grants access?

  If yes, then your system will require the anti-tailgating feature.

- Does a two-person rule apply?

  Under the two-person rule, no individual cardholder may enter an empty controlled area unless accompanied by at least one other person. If a two-person rule applies, the AACS must be programmed to grant access only after verifying both cardholders' credentials.

Tracking Requirements

Tracking what happens at an access control point is important not only at the time an event occurs, but also for future reference, such as when an investigation must be conducted. Tracking requirements to consider when planning an AACS include how the access holder database will be maintained and what types of events the AACS needs to track and maintain.

Life Safety

In addition to planning for entry into a controlled space, you must also take into consideration how people will exit from that space in the event of an emergency. The access control system and door hardware must be able to accommodate free egress or single push for egress under normal circumstances in most cases. These life safety considerations play a role in selecting request-to-exit (REX) devices, such as panic bars, as well as locking mechanisms, so people may exit quickly in the event of an emergency.

Types of Automated Access Control Systems

Types of AACS Overview

Automated access control systems fall into three general types: coded devices, credential devices, and biometric devices. A coded device allows a person to access a controlled area after entering a recognized code or PIN into the device. A credential device allows a person to enter a controlled area after swiping a recognized credential, such as a CAC, in or near the device. A biometric device allows access after a person enters a specific biological characteristic, such as a fingerprint or retina scan, into the device. Now we'll look at each type of AACS in more detail.

Coded Devices

With coded devices, you must enter a recognized code or PIN on a keypad to access a controlled area. Keypad devices are reliable, compact, user-friendly, and easy to maintain, repair, or replace. They are also much less expensive than other types of AACS. Keypad devices do not require individuals to carry cards or tokens, so there is nothing for them to lose. Security personnel can also assign different codes to different points and doors. Keypads may have duress code functionality where a user can covertly enter a special code if forced to enter under duress.

On the other hand, keypad devices do pose some security risks. For example, codes can be easily passed onto unintended or unwelcome visitors. They can be viewed by others and then used for unapproved entry. Finally, keypad devices have a limited number of allowable unique codes. For example, if the device accepts only 4-digit PINs, then there are only 10,000 possible codes.

Credential Devices

Credential devices allow an individual to access a controlled area after swiping a recognized credential in or near the device. There are four types of credentials that are currently in use. One is a smart card or microchip card. A DoD CAC is an example of this type of credential. The other three types are the magnetic stripe card, the proximity card, and the Weigand, or embedded wire, card.

One advantage of credential devices is that cards and card readers are reliable. Among the four types of credential devices, proximity or contactless readers are more convenient than card readers because they require only that a card be placed near the device rather than swiped against or inserted into it. For example, you could leave the card in your purse and just wave your purse near the device.

The disadvantages of credential devices are that cards can be lost or stolen and some types of cards are easy to duplicate. Also, there is mechanical wear on cards that are swiped or inserted versus proximity cards that don’t actually touch a device.

Biometric Devices

Biometric devices allow individuals access to a controlled area after they display a specific biological characteristic into the device, which compares it to a stored characteristic. A variety of biological characteristics are used to identify individuals for authorized access to controlled areas. These include: hand geometry, fingerprint, facial recognition, iris pattern, voice verification, and retinal scanning.

Biometric devices are good because they provide automated verification that the person who is attempting to gain access to a controlled area is authentic. Another positive feature of biometric devices is that biometric credentials are extremely difficult to duplicate. It’s not easy to duplicate someone’s fingerprint!

On the other hand, biometric devices cost more than other types of devices and they take longer to verify an individual. These devices also require special housings, and some of them are not appropriate for outdoor use.

AACS Components

Automated access control systems comprise more than just the access devices or readers you see at doors and other entrances. There are several other components present behind the scenes. For example, credential AACS include equipment to create the badges. And biometric AACS use a biometric template capture device to capture people's biological characteristics, such as fingerprints or retina images.

In addition, each AACS has a central computer or server where the AACS software and database reside that archives all system activity. Each AACS also has a workstation that allows personnel to view and interact with the AACS hardware and software. Authorized personnel use REX devices to exit controlled areas.

Finally, each AACS also has a local processor that collects input from card readers, keypads, biometric devices, door sensors, and REX devices. The local processor uses that input to send signals to electronic door locks, electric door strikes, turnstiles, and gate operators.

Review Activities

Review Activity 1

What can an AACS do to protect assets in a facility?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Allow authorized personnel to enter a controlled area after verifying credentials
- ☐ Assist in preventing unauthorized personnel from entering a controlled area
- ☐ Communicate with CCTV for assessment purposes
- ☐ Communicate with an IDS to sound an alarm to alert security personnel of unauthorized entry attempts

Review Activity 2

Select the best response for each question. Then check your answers in the Answer Key at the end of this Student Guide.

	Coded	Credential	Biometric
A high-security facility requires an AACS that makes it extremely difficult to duplicate the user's form of verification for access. Which type of AACS is most appropriate for that facility?	○	○	○
You have been directed to purchase the least expensive type of AACS for a given facility. Which type of AACS should you choose?	○	○	○
Which type of AACS would allow you to use your CAC as the verification method for authorized entry into a controlled area?	○	○	○

Review Activity 3

Select the best response for each question. Then check your answers in the Answer Key at the end of this Student Guide.

	Two person rule	**Anti-passback**	**REX device**	**Anti-tailgating**
Which AACS feature would you implement to mitigate the risk of someone giving his or her credentials to another person to access a controlled area?	○	○	○	○
Which AACS feature would you implement to prevent individual cardholders from entering a selected empty controlled area unaccompanied?	○	○	○	○
Which AACS feature would you implement to prevent a person from following another person closely in order to gain ingress through the same portal when the authorized person's credential grants access?	○	○	○	○
Which AACS feature would you implement to facilitate egress from a controlled area?	○	○	○	○

Answer Key - Review Activities

Review Activity 1

What can an AACS do to protect assets in a facility?

Select all that apply.

- ☑ Allow authorized personnel to enter a controlled area after verifying credentials
- ☑ Assist in preventing unauthorized personnel from entering a controlled area
- ☑ Communicate with CCTV for assessment purposes
- ☑ Communicate with an IDS to sound an alarm to alert security personnel of unauthorized entry attempts

Feedback*: All of these are ways that an AACS can help protect the assets of a facility.*

Review Activity 2

Select the best response for each question.

	Coded	Credential	Biometric
A high-security facility requires an AACS that makes it extremely difficult to duplicate the user's form of verification for access. Which type of AACS is most appropriate for that facility?	○	○	⊙
***Feedback**: In biometric AACS, it is very difficult to duplicate an authorized individual's form of verification, which is a particular biological characteristic of the individual.*			
You have been directed to purchase the least expensive type of AACS for a given facility. Which type of AACS should you choose?	⊙	○	○
***Feedback**: Coded devices are less expensive than credential and biometric devices.*			
Which type of AACS would allow you to use your CAC as the verification method for authorized entry into a controlled area?	○	⊙	○
***Feedback**: A CAC is a type of verification used on a credential device to access a controlled area.*			

Review Activity 3

Select the best response for each question.

	Two person rule	**Anti-passback**	**REX device**	**Anti-tailgating**
Which AACS feature would you implement to mitigate the risk of someone giving his or her credentials to another person to access a controlled area?	○	⊙	○	○
***Feedback**: Implementing anti-passback will mitigate the risk of someone giving his or her credentials to another person to access a controlled area.*				
Which AACS feature would you implement to prevent individual cardholders from entering a selected empty controlled area unaccompanied?	⊙	○	○	○
***Feedback**: The two-person rule prevents individual cardholders from entering a selected empty controlled area unless accompanied by at least one other person.*				
Which AACS feature would you implement to prevent a person from following another person closely in order to gain ingress through the same portal when the authorized person's credential grants access?	○	○	○	⊙
***Feedback**: Anti-tailgating aims to prevent a person from following another closely to enter through the same portal when the authorized person's credential grants access.*				
Which AACS feature would	○	○	⊙	○

you implement to facilitate egress from a controlled area?				
***Feedback**: Request-to-exit devices ensure that individuals can exit controlled areas.*				

Student Guide

Electronic Security Systems

Lesson 3: Intrusion Detection Systems

Introduction

Objectives

In this lesson, you will learn what intrusion detection systems (IDS) are and the planning considerations for implementing an IDS. You will also learn about the different types of IDS and their components.

Here are the lesson objectives:

- Identify the purpose and role of intrusion detection systems
- Identify key planning considerations for IDS implementation

What Are Intrusion Detection Systems?

Overview of IDS

An IDS is an automated system that detects an intrusion of a specified site, facility, or perimeter and triggers an alarm. An IDS consists of interior or exterior sensors and a premise control unit (PCU).

Planning Considerations

Overview of IDS Planning Considerations

When planning an IDS, there are many factors you need to take into account. These relate to which IDS sensors to use and transmission considerations. Let's take a closer look at each of these considerations.

IDS Sensor Considerations

There are many things you must consider when thinking about what type of sensor to use for an IDS. You should ask yourself these questions.

- What is the probability that this sensor will detect an intrusion, and which types of intrusions?

- Can the sensor be activated by nuisances and weather? How can nuisance and environmental alarms be reduced?
- How much does a particular sensor cost, and how does that compare to the asset being protected?
- What protection is available to protect IDS monitoring equipment, such as equipment racks and electrical equipment rooms?
- Can the sensor be tested remotely to verify sensor operation?
- Is there anything obstructing the sensor from activating?

You must also plan to conduct an acceptance test to ensure the system is working properly once you have had an IDS installed in your facility.

Acceptance Test

Once an IDS has been installed, you must conduct an acceptance test to physically verify that the system is working properly. Here are the steps to conduct an acceptance test. First, you should test the functioning of the PCU and its tamper switch. Next, you should test the functioning of all sensors, switches, and alarms. For example, for doors and windows that have switches, arm the system, then open each door and window to see if that triggers the alarm. Finally, you should test each sensor to discover where the dead zones are. Dead zones are the areas that will not trigger the alarm. If necessary, you will need to adjust the placement of other sensors to cover any dead zones.

Transmission Considerations

For IDS, transmission of data is most important. An IDS sensor will do no good if the status of that sensor is not communicated to the appropriate personnel. Here are the types of things you should consider related to the transmission capability of an IDS.

- What is the expansion capability and bandwidth availability of the transmission system?
- Who will obtain approval of radio frequency emitters by the local jurisdiction or host nation?
- What is needed to protect equipment from tampering, weather, and other factors?
- What coordination of the data transmission media (DTM) transmission lines must take place?

Premise Control Unit

What Is a PCU?

A PCU, also known as an IDS local processor or intrusion panel, is an electronic device that continuously monitors the alarm status of local IDS 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 status via a local keypad, credential reader, or biometric device.

Exterior IDS Sensors

Overview of Exterior IDS Sensors

As you learned, the PCU may connect to external or internal sensors. Exterior IDS sensors come in three general types. Fence-associated sensors detect when an intruder cuts, climbs, or lifts a fence. Buried line sensors are buried underground to detect intruder-induced ground motion. And open terrain, or line-of-sight, sensors detect intruders that cross the sensors' path in open areas. Let's take a closer look at each type.

Pros and Cons of Fence-Associated Sensors

Let's examine the pros and cons of fence-associated sensors.

They are advantageous for their relatively low cost and because they provide overlapping protection across different zones.

However, fence-associated sensors can go off randomly, for example if something heavy strikes the fence. To address this, a best practice is to use a double fence. In this configuration, the sensors are on the inner fence only. The outer fence serves as a barrier for the inner fence to reduce nuisance alarms caused by windblown debris or animals, for example. Fence-application sensors are also vulnerable to intruders who can go under or over fences. An intruder can dig under a fence or build a bridge-like structure over the fence to avoid triggering the sensors.

Types of Fence-Associated Sensors

There are six types of fence-associated sensors.

- Coaxial strain-sensitive cable sensors:
    - Detect mechanical vibrations and wire movement through an electric field
    - Vulnerable to electromagnetic interference
- Time-domain reflectometry (TDR) systems:
    - Send induced radio frequency signals down a cable attached to the fence fabric

    - Detect breaks in radio frequency signals
    - Used on fences not in good condition
- Capacitance proximity sensors:
    - Detect intrusions via a break in the electrical charge between earth ground wires and sensing wires
    - Used on top of fences/roofs/walls
    - Subject to nuisance/environmental alarms
    - Vulnerable to bridging/tunneling
- Fiber optic strain-sensitive cable:
    - Detects motion, vibration, and changes in pressure by detecting changes in interference between modes of light transmitted through the cable
    - Immune to radio frequency interference, lightning, and other sources of electromagnetic interference
- Taut-wire sensors are smooth or barbed wire that:
    - Detect movement through parallel wires under tension
    - Are used on fences/rooftops
    - Have minimal false alarms
    - Are more expensive
    - Require frequent maintenance
    - Are vulnerable to bridging/tunneling
- Electromechanical sensors use switches and coaxial strain-sensitive cable sensors to create an electric field that:
    - Detects mechanical vibrations and movement of wire
    - Detects fence climbing or cutting
    - Are vulnerable to electromagnetic interference
    - Are not recommended for DoD use

Pros and Cons of Buried Line Sensors

As you learned, a second type of exterior sensor for an IDS is a buried line sensor. The primary advantage of buried line sensors is that they are not visible to intruders. On the other hand, buried line sensors are vulnerable to electromagnetic interference (EMI) and intruders can bridge over them to avoid detection. Also, these sensors must be buried to a uniform depth, so they are unreliable in areas prone to ground shifting due to standing water or erosion or to heavy snowfall. The main cause of unreliable detection for buried systems, though, is improper engineering of the burial medium. Loose soil or soil of the wrong consistency and chemistry can attenuate seismic energy before it reaches the sensor.

Types of Buried Line Sensors

There are three types of buried line sensors.

- Ported coaxial cable sensors are good for use in open areas and can be effective as part of a double fence system. They do not work well near electrical substations or other geographic areas with unusual magnetic interference.
- Fiber optic cable sensors are useful in detecting digging and tunneling, so they are good for use in securing pipelines, manholes, and entry portals. They are also useful for vehicle detection at gates and barriers. And they have an interior application as well—in walls. These sensors also are unaffected by metal objects and water.
- Seismic sensors are an effective covert tool against intruders walking, running, digging or operating vehicles or machinery near the detection zone.

Pros and Cons of Open Terrain Sensors

The third type of exterior sensor for an IDS is an open terrain sensor. These are also called line-of-sight sensors. This type of sensor works best on flat, cleared areas. These sensors are best suited for protecting free standing high value assets such as fighter jets. However, because they are out in the open, they are subject to environmental and nuisance alarms, attributed to factors such as overgrown vegetation, snow, the accumulation of standing water and animals.

Open Terrain Sensors

There are four types of open terrain sensors.

- Microwave sensors radiate a controlled pattern of microwave energy into the protected area. If an intruder passes through that microwave energy, it sets off an alarm. There are two types of microwave sensors.
    - Bistatic microwave sensors are used for wide area surveillance of open areas, such as desert environments.
    - Monostatic microwave sensors are used for smaller area surveillance, such as in entry portals. Microwave sensors do not work well around trees or other uncleared areas.
- Infrared sensors project a beam between a sensor and a receiver. These sensors detect intruders who pass through that beam. There are two types of infrared sensors.
    - Active infrared sensors should be projected over a clear path, such as in entry portals.
    - Passive infrared (PIR) sensors work well in exterior environments, such as building perimeters, but only if reflected or radiated light is prevented from interfering.
- Dual-technology sensors combine passive infrared and microwave technology and are effective as gap fillers and should be kept inside a protected area to avoid being compromised.

- Video motion sensors compare successive images from a closed circuit television (CCTV) camera to detect intruders. These types of sensors have both interior and exterior applications.

Interior IDS Sensors

Overview of Interior IDS Sensors

An IDS can also have interior sensors. There are two general types: interior point sensors, which monitor the inside of buildings, generally at entry points such as doors and windows, and interior volumetric sensors, which monitor interior building spaces such as rooms and hallways to detect intruders. Let's take a closer look at each.

Interior Point Sensors

There are four types of interior point sensors.

- Balanced magnetic switch (BMS) / High security switch (HSS)
  - Uses a magnetic field or mechanical contact to determine if an alarm signal is initiated
  - Simplest type
  - Will generate an alarm if tampering occurs where they are installed
  - Use on:
    - Door
    - Window
    - Roof hatch
- Glass break sensors
  - Detect glass breakage
  - Types
    - Shock sensors feel the vibration when glass is broken
    - Acoustic sensors listen for broken glass sound waves
    - Dual-technology sensors are combination of shock and acoustic sensors
  - Use other types of sensors such as volumetric sensors with glass break sensors
- Capacitance sensors
  - Detect changes in capacitance, or electrical charge
  - Isolate assets from ground
  - Adequate ground plane is essential
  - Protect several assets with one sensor
- Pressure sensors
  - Detect weight changes when an asset, such as a safe, is moved off of the sensor
  - Types:

        - Pressure mats detect weight changes on mat
        - Pressure switches detect weight changes when asset (i.e., safe) is moved off switch

Interior Volumetric Sensors

There are four types of interior volumetric sensors.

- PIR sensors
    - Most common interior volumetric sensors
    - Used to detect heat signatures, or infrared emissions, from intruders
    - Work best in an interior climate-controlled environment
- Acoustic sensors
    - Use passive listening devices to monitor building spaces
    - Good for use in office buildings to detect covert intruders who stay behind after business hours
    - Usually used in conjunction with password-protected automated access control systems (AACS) so that when an individual logs into the AACS, the acoustic sensor is disabled
- Dual-technology sensors
    - Use both microwave and PIR technologies to increase probability of detecting intruders
    - Use everywhere, especially in Sensitive Compartmented Information Facilities (SCIFs), vaults, and secure rooms
    - Can be configured to reduce nuisance alarms
- Video motion sensors
    - Were discussed earlier with exterior IDS since they have both interior and exterior applications

Review Activities

Review Activity 1

Select the best response for each question. Then check your answers in the Answer Key at the end of this Student Guide.

	Acceptance test	**Nuisance alarm**	**PCU test**
Which of the following should you conduct to test the placement of IDS sensors?	○	○	○
Which of the following can be caused by an animal activating an IDS sensor?	○	○	○
Which of the following is part of an acceptance test?	○	○	○

Review Activity 2

Select the best response for each question. Then check your answers in the Answer Key at the end of this Student Guide.

	Open terrain sensor	**Buried line sensor**	**Fence-associated sensor**
Which type of exterior IDS sensor is good for detecting intrusion by digging and tunneling?	○	○	○
Which exterior IDS sensor is NOT vulnerable to bridging?	○	○	○
Which exterior IDS sensor is usually the least expensive?	○	○	○
Which exterior IDS sensor is also known as a line-of-sight sensor?	○	○	○

Review Activity 3

Select the best response for each question. Then check your answers in the Answer Key at the end of this Student Guide.

	Balanced magnetic switch (BMS) / High security switch (HSS)	**Glass break sensor**	**Passive infrared sensor**	**Dual-technology sensor**
Which type of sensor would be most effective in protecting a permanently secured window?	○	○	○	○
Which sensor detects heat signatures of intruders and is the most common interior volumetric sensor?	○	○	○	○
Which sensor is used on doors, roof hatches, and windows?	○	○	○	○

Answer Key - Review Activities

Review Activity 1

Select the best response for each question.

	Acceptance test	**Nuisance alarm**	**PCU test**
Which of the following should you conduct to test the placement of IDS sensors?	⊙	○	○
***Feedback**: You should conduct an acceptance test to test the placement of IDS sensors to ensure they are in the proper place and that there are no dead zones.*			
Which of the following can be caused by an animal activating an IDS sensor?	○	⊙	○
***Feedback**: When an animal activates an IDS, it can trigger a nuisance alarm. Similarly, certain weather events can trigger an environmental alarm on an IDS.*			
Which of the following is part of an acceptance test?	○	○	⊙
***Feedback**: In an acceptance test, you should test the functioning of the PCU and all switches, sensors, and alarms.*			

Review Activity 2

Select the best response for each question.

	Open terrain sensor	**Buried line sensor**	**Fence-associated sensor**
Which type of exterior IDS sensor is good for detecting intrusion by digging and tunneling?	○	⊙	○
***Feedback**: The fiber optic cable sensor is a buried line sensor that is effective in detecting digging and tunneling.*			
Which exterior IDS sensor is NOT vulnerable to bridging?	⊙	○	○
***Feedback**: Buried line and fence-associated sensors are both vulnerable to bridging. Open terrain sensors are not.*			
Which exterior IDS sensor is usually the least expensive?	○	○	⊙
***Feedback**: Fence-associated sensors are generally the least expensive types of exterior sensors.*			
Which exterior IDS sensor is also known as a line-of-sight sensor?	⊙	○	○
***Feedback**: Open terrain sensors are also called line-of-sight sensors.*			

Review Activity 3

Select the best response for each question.

	Balanced magnetic switch (BMS) / High security switch (HSS)	**Glass break sensor**	**Passive infrared sensor**	**Dual-technology sensor**
Which type of sensor would be most effective in protecting a permanently secured window?	○	⊙	○	○
***Feedback**: A glass break sensor would be the most effective sensor for a permanently secured window because the intruder would most likely have to physically break the window to enter.*				
Which sensor detects heat signatures of intruders and is the most common interior volumetric sensor?	○	○	⊙	○
***Feedback**: Passive infrared sensors detect heat signatures of intruders. They are the most common interior volumetric sensor.*				
Which sensor is used on doors, roof hatches, and windows?	⊙	○	○	○
***Feedback**: Balanced magnetic switches (BMS) or high security switches (HSS) are used on doors, roof hatches, and windows.*				

Student Guide

Electronic Security Systems

Lesson 4: Closed Circuit Television Systems

Introduction

Objectives

In this lesson, you will learn what closed circuit television (CCTV) systems are, as well as the planning considerations for implementing a CCTV system. You will also learn about the different CCTV system components.

Here are the lesson objectives:

- Identify the purpose and role of closed circuit television (CCTV) systems
- Identify key planning considerations for CCTV implementation

CCTV Systems Overview

What Are CCTV Systems?

A CCTV is an automated system that can view, monitor, and record security events. CCTV systems can be used both indoors and outdoors.

Capabilities of CCTV Systems

CCTV systems have four primary capabilities.

First, they can help assess the validity of alarms. Connecting a CCTV system to an intrusion detection system (IDS) alarm allows security personnel to visually assess a situation to determine what type of response may be required.

Second, they can help with access control. Connecting a CCTV system to an automated access control system (AACS) allows security personnel to visually identify persons and vehicles requesting entry before they release a controlled portal, such as a door, turnstile, gate, or vehicle barrier.

Third, CCTV systems perform a surveillance function. They enable security personnel to view events at multiple locations from a centralized remote viewing area. CCTV cameras posted in various areas help to deter loss, theft, and unauthorized entry.

Finally, CCTV systems can archive information for use as evidence. They allow security personnel to retrieve images that may provide evidence of security breaches. This can help identify or prosecute trespassers, vandals, or other intruders.

Planning Considerations

When planning a CCTV, there are a variety of factors to consider.

- Do you intend to use the CCTV system indoors or outdoors? And how do you intend to use it? For example, do you plan to pair it with an AACS or an IDS?
- You must also consider the lighting in the area where you plan to operate the CCTV system. Will it be working in broad daylight? In complete darkness? Both?
- Finally, you need to think about physical obstacles that could block the camera's view of an area. For example, are there trees or vegetation between the camera and the area you want to observe?

CCTV Components

Overview

CCTV systems are comprised of cameras, which take in the surveillance data; recorders, which store that data; and workstations, which allow personnel to view, organize, and manipulate the data. Let's take a look at each component.

Camera Types: Fixed vs. Moveable

Selecting the right CCTV camera is crucial to CCTV system design. CCTV cameras come in many forms and have various options that serve different purposes. Let's take a look at the different options a CCTV camera can have.

Cameras can be either fixed, meaning they focus on one position, or moveable, meaning they focus on different areas through remote control. This movable feature is referred to as pan, tilt, and zoom (PTZ).

Fixed cameras are better suited for assessing alarms on doors, gates, and fence lines; to go back and review a scene before an alarm occurred; and to detect motion. PTZ cameras, on the other hand, are better suited for surveillance of large open areas, such as ports and airfields. Also, PTZ cameras can follow the path of an intruder. However, PTZ cameras are more expensive than fixed cameras.

Camera Features

Identifying which features you need your CCTV camera to have depends on a variety of factors.

- First, what area do you want your CCTV system to oversee? How large is it? The size of the area will determine the kind of lens you want to use. For example, a wide-angle lens is best for a large surveillance area.

  The type of area you need to survey will also help determine where you should mount the camera. How high up does it need to be?

- Next, where will you locate the camera? Whether the camera will be indoors or outdoors will determine whether you need protective housing, and if so, what kind.

  The camera location also defines your lighting requirements. How dark is the area it covers? What times of day will the system be recording? Different camera features are better for different lighting situations.

- Do you need to conceal the camera? If so, you might consider using a dome to hide the lens.

- Finally, should you use a color or a black-and-white camera?

  Color cameras require higher illumination and provide more detail, such as the color of clothing an intruder is wearing, than black and white cameras provide.

  Black-and-white cameras work better than color cameras in low-light conditions.

Low-light features

For conditions in which there is low light, or even no light, there are some options to enable camera surveillance.

Infrared (IR) illuminators enable cameras to record images in little or no light. IR illuminators use infrared light to allow night surveillance without artificial lighting. And the human eye cannot see the infrared light they emit.

Thermal imagers operate in complete darkness. They do this by sensing the heat signatures that objects, such as people, emit. Thermal imagers are less vulnerable to environmental factors such as rain and fog. However, they are relatively expensive and do not provide the same level of detail in their images as those from visible light cameras.

Recorders

CCTV systems employ two different types of recorders: digital video recorders (DVRs) and network video recorders (NVRs).

DVRs digitize multiple analog camera inputs and store the video on internal hard drives. DVRs are good for most security applications, including assessing alarms and storing evidentiary archives. They can record up to 30 frames per second.

NVRs record digital video from multiple cameras to internal hard drives. NVRs are best for surveillance applications because they allow an operator to see a smooth video stream. To do this, they can record up to 60 frames per second. NVRs require a high-speed network.

According to the National Archives and Records Administration (NARA) General Records Schedule (GSRS) 21, under the Authority: 44 U.S.C 3105, 3106 and 36 CFR Part 1230 Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records, routine surveillance recordings must be maintained for 6 months. Waivers must be processed through Agency's Records Management offices and approved by NARA.

Workstation

CCTV workstations allow personnel to view both live and recorded video. CCTV workstations include monitors, keyboards, and graphics cards. They may also include joysticks for controlling PTZ cameras, video management software, and video analytics software. Video analytics software lets a user input a set of rules for each scene of interest. If a rule is violated, a visual cue displays on the monitor, which draws the operator’s attention to suspicious objects and behaviors. For example, you could set a rule to create an alert if the camera detects any movement in a sensitive area where there is not supposed to be any movement.

Review Activities

Review Activity 1

For each statement, select which CCTV system capability it demonstrates. Then check your answers in the Answer Key at the end of this Student Guide.

	Access Control	**Alarm Assessment**	**Surveillance**
Monitoring a military exchange	○	○	○
Viewing a CCTV monitor to determine security force response to an alarm	○	○	○
Viewing individuals on a CCTV camera to grant or deny access to a facility	○	○	○

Review Activity 2

You have received a request to add a CCTV system to a building on your installation. Which questions should you ask?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Will the CCTV system be used inside or outside?
- ☐ Will the CCTV system be used in a very well-lit area, in low lighting, or in the dark?
- ☐ Are there any visual obstacles that might block the system from capturing clear images?
- ☐ Will the system require a person to man the monitor at all times?

Answer Key - Review Activities

Review Activity 1

For each statement, select which CCTV system capability it demonstrates.

	Access Control	Alarm Assessment	Surveillance
Monitoring a military exchange	○	○	⊙
***Feedback**: CCTV systems enable security personnel to conduct surveillance of multiple locations from a centralized remote viewing area.*			
Viewing a CCTV monitor to determine security force response to an alarm	○	⊙	○
***Feedback**: Connecting a CCTV system to an IDS alarm allows security personnel to visually assess a situation to determine what type of response may be required.*			
Viewing individuals on a CCTV camera to grant or deny access to a facility	⊙	○	○
***Feedback**: Connecting a CCTV system to an AACS allows security personnel to visually identify persons and vehicles requesting entry before they release a controlled portal, such as a door, turnstile, gate, or vehicle barrier.*			

Review Activity 2

You have received a request to add a CCTV system to a building on your installation. Which questions should you ask?

Select all that apply.

- ☑ Will the CCTV system be used inside or outside?
- ☑ Will the CCTV system be used in a very well-lit area, in low lighting, or in the dark?
- ☑ Are there any visual obstacles that might block the system from capturing clear images?
- ☑ Will the system require a person to man the monitor at all times?

Feedback*: You should ask all of these questions before planning a CCTV system.*

Student Guide

Electronic Security Systems

Lesson 5: Data Transmission Media

Introduction

Objectives

In this lesson, you will learn what data transmission media (DTM) links are, including the different types of DTM. You will also learn the key planning considerations for implementing a DTM.

Here are the lesson objectives:

- Identify the purpose and role of data transmission media (DTM) for electronic security systems (ESS)
- Identify key planning considerations for DTM implementation

DTM Overview

An effective data transmission media link allows for rapid and reliable data transmission and communication among ESS subsystems, from intrusion detection sensors, access control devices, and video components to display and assessment equipment. The DTM also transmits data between the ESS subsystems and the dispatch or control center to alert the security forces of any alarm conditions. An effective DTM link is resistant to compromise, has redundancy, and is conducive to rapid fault detection and repair.

Planning Considerations

What You Should Consider for DTM

When planning DTM links, you must consider connectivity requirements, such as bandwidth, pathways, power sources, and secure communications. You must also think about the best ways to have the ESS subsystems communicate with each other. Let’s take a look at the types of things you need to think about for each.

Connectivity Requirements

When thinking about connectivity requirements, you must identify how much bandwidth each subsystem will require under normal conditions and under high-traffic conditions to determine how much bandwidth you will need. CCTV systems generally require the most bandwidth, whereas IDS generally require the least.

For connectivity of DTM links to be effective, they must use a power source that cannot be interrupted. Therefore, there should always be an emergency power source to use as backup if the primary source fails.

You must also think about how the subsystems will connect to each other. Can they connect to existing networks or do you need to create new pathways?

Finally, DTM links require secure communications. To accomplish this, you must consider physical protections, such as conduits for conductors to guard against environmental factors, and electronic protections, such as encryption to guard against hackers.

Integrating Subsystem Communication

When planning DTM links, you must consider various factors that go into integrating the communications between the ESS subsystems. Here are some examples.

- When the IDS and AACS are separate, it is preferable to use one single door sensor with two independent outputs rather than two separate sensors. This reduces costs and eliminates clutter.
- To connect an IDS to a CCTV or a CCTV to an AACS, use hardwired conductors for simple installations.
- To reduce wiring costs, serial communications can use a single serial data link to handle several camera control signals.
- For most projects, you should use software-based integration to connect the systems. This provides flexibility in the initial system setup and allows users to make configuration changes with no additional hardware or wiring. To do this, you need a networked ESS system and a dedicated security network. And again, the same vendor must manufacture both systems, or you will need a software driver.
- For communication from an AACS to a dispatch center, the monitored facility must have a local processor that is compatible with the existing central monitoring system.

DTM Links

DTM Infrastructure

The infrastructure available at a facility will determine the type of DTM link you use. The DTM infrastructure mandates who controls the DTM link and what security measures may be required to secure the DTM link.

One type of DTM infrastructure refers to DTM links, which are located completely on Department of Defense (DoD) proprietary or leased property. This type is referred to as Base Level Information Infrastructure (BLII) or on-base communications. For example, the DTM link that carries the data and communication between the ESS subsystems on a military installation and the control center that is also located on that installation would be considered a BLII, or on-base communications.

The other type of DTM infrastructure refers to those DTM links that are not located completely on DoD proprietary or leased property. This type is referred to as Defense Information Infrastructure (DII) or inter-base communications. So, for example, the DTM link that carries the data and communications between the ESS subsystems in a DoD building and a private security company that is not located on DoD property but that monitors the DoD building's security is a DII, or inter-base communications.

DTM Networks

DTM links transmit data over DTM networks. You may use different types of DTM networks depending on your operating infrastructure and the level of security you need. Using hardwired networks is the most secure way to transmit data, but sometimes you will need to use wireless networks to communicate over areas where it is difficult to lay hardwired networks.

There are two types of hardwired networks. Dedicated conductors are dedicated proprietary, or DoD-owned, circuits that transmit data and video between DTM nodes. Direct subscriber lines, also known as T-1 lines, are permanent point-to-point links through public networks. T-1 lines are uniquely assigned to a customer. For example, only DoD information would be transmitted over a DoD entity's assigned point-to-point link. T-1 lines are primarily used in DTM links for connecting remote sites.

Wireless networks are less secure than hardwired networks because they use radio frequency (RF) to transmit data over barriers. Wireless networks are vulnerable to interception, radio frequency interference (RFI) and climatic conditions.

Types of Hardwired DTM

There are three types of hardwired DTM.

The preferred hardwired DTM is fiber optic cable. This cable can transmit data over longer distances and it has a high bandwidth. It uses infrared or visible light through transparent fibers. Fiber optic is not vulnerable to electromagnetic interference (EMI) to RFI, or to lightning. However, fiber optic is susceptible to breakage due to cable stress, stretching, and bending. It is also the most expensive type of hardwired DTM.

Coaxial cable is good for CCTV systems, high-speed data transmissions, and transmission of simultaneous voice conversations. Like fiber optic, coaxial cable also has a high bandwidth. It also provides good isolation from external noise and crosstalk.

Wireline can meet most ESS data transmission needs but has limited bandwidth. Also, unlike fiber optic, coaxial cable and wireline are vulnerable to EMI, RFI, and lightning, but these vulnerabilities can be reduced if they are grounded at one end or shielded.

Review Activities

Review Activity 1

Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	True	False
A wireless network is more secure than a hardwired network.	○	○
Software-based integration is the preferred DTM method for most projects.	○	○
A DTM allows an automated access control system to communicate with a control center.	○	○
Wireline DTM, which is good for most ESS data transmission needs, has a high bandwidth.	○	○

Review Activity 2

Which of the following are considerations when planning for a DTM link?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ What is the bandwidth of each ESS subsystem being connected?
- ☐ What level of security will be required?
- ☐ Is there an uninterruptible power supply?
- ☐ Can you use existing networks or will you need to create a new pathway?

Answer Key - Review Activities

Review Activity 1

Select True or False for each statement.

	True	False
A wireless network is more secure than a hardwired network.	○	○
***Feedback**: Hardwired networks are more secure and the least likely to be intercepted. Wireless networks, although best suited for communication over barriers, are more vulnerable to interception than hardwired networks.*		
Software-based integration is the preferred DTM method for most projects.	○	○
***Feedback**: Software-based integration is the preferred DTM method for most projects.*		
A DTM allows an automated access control system to communicate with a control center.	○	○
***Feedback**: A DTM allows any ESS subsystem to communicate with each other and a control center.*		
Wireline DTM, which is good for most ESS data transmission needs, has a high bandwidth.	○	○
***Feedback**: Wireline is good for most ESS data transmission needs, but it has a limited bandwidth. Both fiber optic cable and coaxial cable have a high bandwidth.*		

Review Activity 2

Which of the following are considerations when planning for a DTM link?

Select all that apply.

- ☑ What is the bandwidth of each ESS subsystem being connected?
- ☑ What level of security will be required?
- ☑ Is there an uninterruptible power supply?
- ☑ Can you use existing networks or will you need to create a new pathway?

***Feedback**: All of these are items you must consider when planning for a DTM link.*

Student Guide

Electronic Security Systems

Lesson 6: Monitoring Methods

Introduction

Objectives

In this lesson, you will learn about the four main types of monitoring methods electronic security systems (ESS) use. You will also learn about the pros and cons in planning for each ESS monitoring method.

Here are the lesson objectives:

- Identify the purpose and role of monitoring methods for ESS
- Identify key planning considerations for implementation of ESS monitoring

Overview of Monitoring Methods

For an ESS to be effective, someone or something needs to monitor the alarms it generates. Without this capability, the system is unable to perform its function—to prevent unauthorized access. Facilities use trained personnel, generally 24 hours per day, seven days per week, to centrally monitor and assess the automated access control systems, closed circuit television systems, and intrusion detection systems at the facility. Four ways that security forces monitor electronic security systems are through proprietary station, local alarm, central station, and police connection. Let's take a closer look at each type of monitoring method.

Proprietary Station Monitoring

Features

With the proprietary station method, a facility monitors alarms using its own facilities, equipment, and staff and the installation's security force responds to all ESS alarms. This is the preferred and most common method used on DoD installations.

Planning Considerations

Here are some things to think about when planning for proprietary station monitoring.

The primary advantage of using a proprietary station for monitoring an ESS is that it does not rely on outside sources. It uses a facility's own space, equipment, and staff. Also, the ESS can include closed circuit television (CCTV) monitoring for alarm assessment, video analytics, and general surveillance.

The disadvantages of proprietary station monitoring relate primarily to expenses. These include a possible need to increase staffing so trained personnel are available around the clock, and the ongoing labor cost for the dispatch center operators. Also, a proprietary station requires the facility to provide real estate space and equipment for the monitoring station.

Local Alarm Monitoring

Features

Local alarm monitoring relies on security forces in the immediate area to respond to visual or audible alarm signals. These alarms are usually located on the exterior of a facility, but the transmission lines stay within the facility. Because the primary purpose of local alarms is to deter intruders, they should always be used in conjunction with another type of monitoring.

Planning Considerations

When deciding whether to employ local alarm monitoring, its advantages are that it is easy to implement and is cost effective. However, since local alarm monitoring relies on security personnel hearing or seeing an alarm, there is no guarantee that an alarm will receive a response if security personnel are not in visual or audible range of the sounding alarm.

Central Station Monitoring

Features

With central station monitoring, a commercial firm monitors facility alarms with around-the-clock operators, and also provides the response forces. The connection between the central station and the alarms being monitored at a facility is usually over leased telephone lines.

Planning Considerations

A major advantage of central station monitoring is that it does not require any additional real estate space or buildings, as does a proprietary station. Unlike both proprietary station and local alarm monitoring, central station monitoring most likely will not require any additional staffing. However, central station monitoring does require an existing central station, which may not be available in all locations. In addition, the company that owns the central station will require payment for monitoring services. Another disadvantage is that establishing connections between

the central station and the facility being monitored can be complex. Also, the central station may rely on non-DoD forces to both monitor and respond to alarms. Finally, with central station monitoring, CCTV capability may be limited or nonexistent.

Police Connection Monitoring

Features

With police connection monitoring, a local police agency dispatch center monitors alarms for a facility. Police personnel respond to the alarms. Police connection monitoring requires a formal agreement between the facility being monitored and the police department. The connection to the police station is usually over leased telephone lines. This type of monitoring is typically used to protect remote facilities and other high-value assets that are not located on a DoD facility or installation.

Planning Considerations

The biggest advantage of police connection monitoring is that the facility being monitored has direct communication with law enforcement. This means the facility could receive a faster police response since there is no middleman between the facility and the response force. However, the police response time would depend on the priorities of the responding law enforcement agency.

As with central station monitoring, police connection monitoring does not require any additional real estate space or building expense. And police connection monitoring does not usually require any additional staffing on the part of the facility being monitored.

However, also like central station monitoring, police connection monitoring may require payment of an ongoing fee. Police connection monitoring usually does not have CCTV assessment capability, nor does it have an archiving resource, so you would need to consider having a separate archiving resource. It also requires an interface connection.

Finally, because police departments may impose penalties for false alarms above a certain threshold, facilities sometimes turn down the sensitivity on their systems. Although this minimizes nuisance alarms, it can result in missed detections of intrusions.

Review Activities

Review Activity 1

Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	True	False
Police connection and central station monitoring generally require an increase in staffing at the facility being monitored.	○	○
Proprietary station monitoring is the method used most by DoD installations.	○	○
Police connection and central station monitoring are generally connected to the facility being monitored through leased telephone lines.	○	○
Local alarm monitoring works best without another type of monitoring used in conjunction with it.	○	○

Review Activity 2

Select the type of monitoring that best matches each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	Proprietary Station	**Local Alarm**	**Central Station**	**Police Connection**
A facility owns and operates the dispatch center and security forces.	○	○	○	○
The local police agency monitors a facility's alarms.	○	○	○	○
Owned by a commercial firm and not usually located on the facility being monitored.	○	○	○	○
Requires roving security forces.	○	○	○	○

Answer Key - Review Activities

Review Activity 1

Select True or False for each statement.

	True	False
Police connection and central station monitoring generally require an increase in staffing at the facility being monitored.	○	⊙
***Feedback**: Police connection and central station monitoring do not generally require an increase in staffing at the facility being monitored. However, local alarm and proprietary monitoring do generally require an increase in staffing.*		
Proprietary station monitoring is the method used most by DoD installations.	⊙	○
***Feedback**: Proprietary station monitoring is the method used most by DoD installations.*		
Police connection and central station monitoring are generally connected to the facility being monitored through leased telephone lines.	⊙	○
***Feedback**: Police connection and central station monitoring are generally connected to the facility being monitored through leased telephone lines.*		
Local alarm monitoring works best without another type of monitoring used in conjunction with it.	○	⊙
***Feedback**: Local alarm monitoring works best when used in conjunction with another type of monitoring.*		

Review Activity 2

Select the type of monitoring that best matches each statement.

	Proprietary Station	**Local Alarm**	**Central Station**	**Police Connection**
A facility owns and operates the dispatch center and security forces.	⊙	○	○	○
***Feedback**: In proprietary station monitoring, a facility owns and operates the dispatch center and security forces.*				
The local police agency monitors a facility's alarms.	○	○	○	⊙
***Feedback**: In police connection monitoring, the local police agency monitors a facility's alarms, and police personnel respond to alarms.*				
Owned by a commercial firm and not usually located on the facility being monitored.	○	○	⊙	○
***Feedback**: In central station monitoring, a commercial firm owns and operates the central station, which is not usually located on the facility being monitored.*				
Requires roving security forces.	○	⊙	○	○
***Feedback**: Local alarm monitoring requires roving security forces to hear or see and respond to audible or visual alarms.*				

Student Guide

Electronic Security Systems

Lesson 7: Putting It All Together

Introduction

Objectives

In this lesson, you will learn about different ways of integrating all of the electronic security systems (ESS) you learned about, as well as the baseline requirements for specific areas that require ESS protection.

Here is the lesson objective:

- Apply the baseline requirements for electronic security systems (ESS) for Sensitive Compartmented Information Facilities (SCIFs), Top Secret/Secret open storage areas, arms storage areas/armories, and magazines

ESS Subsystem Integration

Security in Depth

The most effective way you can protect any asset is by providing more than one type of protection for it. The best approach is to start in the area closest to the asset and move outward, adding layers of protection in areas farther from the asset. This important physical security concept is known as security in depth. This lesson will focus on security in depth specific to ESS.

Types of ESS

As you learned, while ESS subsystems can stand alone, they are usually used in combination with other ESS subsystems. The ways you can integrate them range from the very simple, using only a single system, to the complex, networking an array of ESS subsystems.

The simplest type of ESS contains only a single ESS subsystem, such as an intrusion detection system (IDS) by itself.

An intermediate system contains elements of at least two ESS subsystems that require integration, such as an automated access control system (AACS), and an IDS, communicating directly to a dispatch center.

The third type of ESS is a complex system. Complex systems have separate AACS and IDS communicating with each other, as well as closed-circuit television (CCTV) systems, communicating with the AACS. All three of these communicate to a dispatch center through a data transmission media (DTM) link.

The most complex type of ESS is a networked system. A networked system operates on a single network with drivers to the discrete components of each subsystem. It is a completely self-contained dedicated local area network (LAN) with security system software installed and run on a host server. If a networked system is ever connected to an outside LAN or wide area network (WAN), then you must use additional security measures.

ESS Baseline Requirements

Overview of ESS Baseline Requirements

Certain types of areas have special protection requirements. Area-specific guidance documents detail the requirements that apply to each. You must also consult any Component-specific guidance that applies to your situation. For the rest of this lesson we will use a fictional military installation, Ft. Bravo, to examine the baseline ESS requirements for a Sensitive Compartmented Information Facility (SCIF), a Top Secret and Secret collateral open storage area, an arms room or armory, and a magazine.

SCIFs

When you are planning the ESS for a SCIF, refer to these documents:

- ICS 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities
- IC Tech Spec for ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities
- DoDM 5105.21, Vol. 103, Sensitive Compartmented Information Administrative Security Manual
- Unified Facilities Criteria (UFC) 4-021-02, Electronic Security Systems
- UFC 4-010-05, Sensitive Compartmented Information Facilities Planning, Design and Construction

Here is a summary of the baseline requirements for each ESS subsystem protecting a SCIF.

Access Control

Access control to a SCIF requires:

- Card reader with keypad at primary entrance
- Electric door strikes installed in conjunction with AACS and be UL 1034 Listed for burglar resistance
- Equipment containing access control software programs (PCU) must be located inside the SCIF

Intrusion Detection System

When a SCIF is not continuously manned or under constant surveillance, the SCIF must be protected by an IDS, and the following requirements apply:

- IDS must be independent of systems safeguarding other facilities
- IDS must be compatible with installation's central monitoring system
- All sensors, PCUs, and IDS/AACS admin workstations must be located within SCIF perimeter
- Point sensors on all doors and man-passable openings must meet specific requirements
- Motion sensors to protect windows, doors, and man-passable openings and to detect movement
- Motion sensors not required above false ceilings or below false floors but may be required for critical and high threat facilities outside the U.S.
- Emergency exit doors secured, alarmed, and monitored 24/7
- Interior areas (including walls common to areas not protected at SCI level) protected by IDS consisting of motion sensors and high-security switches
- IDS must have continuously monitored tamper detection devices and transmit alarm condition to PCU or monitoring station
- Must have emergency backup power that does not trigger alarm but that provides visual indicator on PCU and notifies monitoring station of change in power source

Closed Circuit Television

- No CCTV cameras within the SCIF
- External CCTV camera may be used to monitor primary entrance by SCI-indoctrinated personnel within the SCIF

Data Transmission Media

- Requirements for system-associated cabling that extend beyond SCIF perimeter:
    - Rigid conduit installation with dielectric breaks
    - Line supervision or two independent means of transmitting alarm signal to monitoring location
    - NIST FIPS 140-2 encryption; alternative methods must be approved by the Accrediting Official (AO)
- Cabling between all sensors and PCU must be dedicated to the system and contained within the SCIF; if cabling cannot be contained within SCIF, it must meet requirements for External Transmission Line Security

Top Secret/Secret Open Storage Area

When you are planning the ESS for a Top Secret or Secret collateral open storage area, refer to these documents:

- DoD 5200.01-M, Volume 3, DoD Information Security Program
- Unified Facilities Criteria (UFC) 4-021-02, Electronic Security Systems
    - Appendix C contains the baseline requirements

Here is a summary of the baseline requirements for each ESS subsystem protecting a Top Secret or Secret collateral open storage area.

Access Control

Access control to a TS/S open storage area requires:

- Visual recognition or
- Mechanical/automated access control devices

Intrusion Detection System

When a TS/S open storage area is not continuously manned or under constant surveillance, a Top Secret/Secret open storage area must be protected by an IDS, and the following requirements apply:

- All sensors and PCUs located within the protected area perimeter
- Motion sensors and high-security switches to protect perimeter doors and man-passable openings
- IDS installed in accordance with specific requirements
- Dual-technology sensors authorized as long as each technology transmits alarm conditions independent of the other technology

- IDS and any connected AACS equipped with continuously monitored tamper detection devices that transmit alarm condition to PCU or monitoring station
- Emergency exit doors secured, alarmed, and monitored 24/7

When continuously manned, the protected area should be equipped with an alerting system on all potential entrances into the protected area that cannot be observed by the occupants.

Closed Circuit Television

- No CCTV cameras in spaces that contain classified material
- External CCTV camera may be used to monitor primary entrance

Data Transmission Media

- Requirements for system-associated cabling that extends beyond protected area perimeter:
  - Rigid conduit installation
  - Line supervision or two independent means of transmitting alarm signal to monitoring location
  - NIST FIPS 140-2 encryption
- Cabling between all sensors and PCU must be dedicated to the system and contained within the protected area

Arms Storage/Armories

When planning an ESS for arms storage areas and armories, refer to these documents:

- DoD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- Unified Facilities Criteria (UFC) 4-021-02, Electronic Security Systems
  - Appendix C contains the baseline requirements

Here is a summary of the baseline requirements for each ESS subsystem protecting an arms room or armory.

Access Control

- No AACS required
- Requires a high-security padlock with a hasp

Intrusion Detection System

When not continuously manned or under constant surveillance, an arms storage area or armory must be protected by an IDS, and the following requirements apply:

- All sensors and PCUs located within the protected area perimeter
- Motion sensors and high-security switches to protect perimeter doors and man-passable openings
- Duress alarms at all issue ports
    - Duress alarm devices consist of two types (fixed and portable) and are usually manually activated. Fixed are operated using finger, hand or foot, whereas, portable have a transmitter and receiver. When someone under duress activates the alarm, the duress alarm initiates an alarm condition at the central monitoring station and does not result in an audible or visual signal in the protected area.
- Keypad at entrance and for all separate (unit-based) interior storage areas that require an independent IDS capability
- Perimeter emergency exit doors secured, alarmed, and monitored 24/7
- IDS and any connected AACS equipped with continuously monitored tamper detection devices that transmit alarm condition to PCU or monitoring station
- IDS installed in accordance with specific requirements

Closed Circuit Television

- Must be integrated with IDS

Data Transmission Media

- Requirements for system-associated cabling that extends beyond protected area perimeter:
    - Rigid conduit installation
    - Line supervision or two independent means of transmitting alarm signal to monitoring location
    - NIST FIPS 140-2 encryption
- Cabling between all sensors and PCU must be dedicated to the system and contained within the protected area

Magazines and AA&E Facilities

When planning an ESS for magazines and AA&E facilities, refer to these documents:

- DoD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- Unified Facilities Criteria (UFC) 4-021-02, Electronic Security Systems
    - Appendix C contains the baseline requirements

Here is a summary of the baseline requirements for each ESS subsystem protecting a magazine or AA&E facility.

Access Control

- No AACS required
- Requires a high-security padlock with a hasp

Intrusion Detection System

When not continuously manned or under constant surveillance, a magazine or AA&E facility must be protected by an IDS, and the following requirements apply:

- All sensors and PCUs located within the protected area perimeter
- Motion sensors and high-security switches to protect perimeter doors and man-passable openings
- Keypad at entrance and for all separate (unit-based) storage areas that require an independent IDS capability
- IDS and any connected AACS equipped with continuously monitored tamper detection devices that transmit alarm condition to PCU or monitoring station
- IDS installed in accordance with specific requirements

Security Risk Category (SRC) I and II AA&E facility additional requirements:

- Perimeter emergency exit doors must be secured, alarmed, and monitored 24/7
- Vibration sensors on walls to detect boundary penetration attempts
- Duress alarms at all issue ports
    - Duress alarm devices consist of two types (fixed and portable) and are usually manually activated. Fixed are operated using finger, hand or foot, whereas, portable have a transmitter and receiver. When someone under duress activates the alarm, the duress alarm initiates

an alarm condition at the central monitoring station and does not result in an audible or visual signal in the protected area.

Closed Circuit Television

- CCTV, when required, must be integrated with IDS

Data Transmission Media

- Requirements for system-associated cabling that extends beyond protected area perimeter:
    - Rigid conduit installation
    - Line supervision or two independent means of transmitting alarm signal to monitoring location
    - NIST FIPS 140-2 encryption
- Cabling between all sensors and PCU must be dedicated to the system and contained within the protected area

Review Activity

Review Activity

You need to plan the ESS for various special areas in a new facility.

1 of 4: Which of the following require(s) a mechanical/automated access control system or visual recognition as the access control method?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ SCIF
- ☐ Top Secret/Secret collateral open storage area
- ☐ Arms room
- ☐ Magazine

2 of 4: Which of the following may contain a CCTV within the protected area?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ SCIF
- ☐ Top Secret/Secret collateral open storage area
- ☐ Arms room
- ☐ Magazine

3 of 4: Which of the following must have vibration sensors on its walls to detect boundary penetration attempts?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ SCIF
- ☐ Top Secret/Secret collateral open storage area
- ☐ Arms room
- ☐ Magazine

4 of 4: Which of the following require(s) any system-associated cabling that extends beyond protected area perimeter to be installed in rigid conduit?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ SCIF
- ☐ Top Secret/Secret collateral open storage area
- ☐ Arms room
- ☐ Magazine

Answer Key - Review Activity

Review Activity

You need to plan the ESS for various special areas in a new facility.

1 of 4: Which of the following require(s) a mechanical/automated access control system or visual recognition as the access control method?

Select all that apply.

- ☐ SCIF
- ☑ Top Secret/Secret collateral open storage area
- ☐ Arms room
- ☐ Magazine

Feedback: *Top Secret/Secret collateral open storage areas require visual recognition or a mechanical or automated ACS device, while SCIFs, arms rooms and magazines do not have this requirement. Instead, SCIFs require a card reader with a keypad and arms rooms and magazines require the use of a high-security padlock with a hasp to control access.*

2 of 4: Which of the following may contain a CCTV within the protected area?

Select all that apply.

- ☐ SCIF
- ☐ Top Secret/Secret collateral open storage area
- ☑ Arms room
- ☑ Magazine

Feedback: *CCTV cameras are not allowed inside any areas that contain classified information. CCTV cameras are permitted inside arms rooms and magazine and must be integrated with the IDS for those areas.*

3 of 4: Which of the following must have vibration sensors on its walls to detect boundary penetration attempts?

Select all that apply.

- ☐ SCIF
- ☐ Top Secret/Secret collateral open storage area
- ☐ Arms room
- ☑ Magazine

Feedback: *A magazine, if it is classified as a Security Risk Category (SRC) I or II AA&E facility, must have vibration sensors on its walls to detect boundary penetration attempts. These other special areas do not have this as a baseline ESS requirement.*

4 of 4: Which of the following require(s) any system-associated cabling that extends beyond protected area perimeter to be installed in rigid conduit?

Select all that apply.

- ☑ SCIF
- ☑ Top Secret/Secret collateral open storage area
- ☑ Arms room
- ☑ Magazine

Feedback: *All of these areas have this and other DTM requirements for any system-associated cabling that extends beyond the protected area perimeter.*

Student Guide

Electronic Security Systems

Lesson 8: Course Conclusion

Course Conclusion

Course Summary

In this course, you learned about the electronic security systems (ESS) we use to protect our military installations and DoD facilities. You learned about the different subsystems that compose ESS: automated access control systems, intrusion detection systems, closed circuit television systems, data transmission media, and monitoring centers.

Course Objectives

Congratulations. You have completed the Electronic Security Systems course. You should now be able to:

- Define the purpose of electronic security systems (ESS)
- Identify the purpose and roles of the subsystems that compose ESS
- Identify applicable references and policies for specific types of and best uses for ESS
- Apply the baseline requirements for ESS for Sensitive Compartmented Information Facilities (SCIFs), Top Secret/Secret open storage areas, conventional arms storage areas/armories, and magazines
- Identify key planning considerations for ESS implementation

To receive course credit, you **MUST** take the Electronic Security Systems examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.