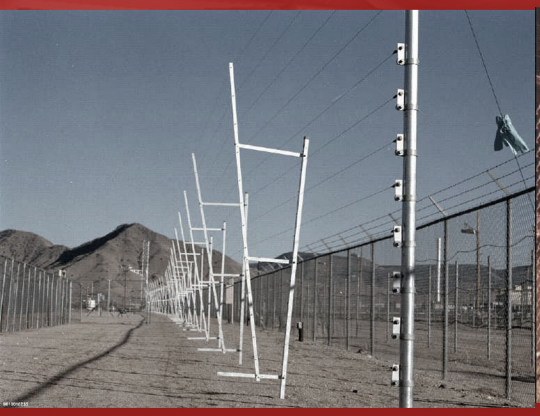
SAND2010-5977P

Infrastructure Development: Initiating a Physical Protection Program



Sandia National Laboratories

National Nuclear Security Administration

SAND 12345678

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-

This page intentionally left blank.

Initiating a Physical Protection Program

Table of Contents

This page intentionally left blank.

Infrastructure Development: Initiating a Physical Protection Program

Module 1:
Introduction and Overview

1

Module Objectives

- Introductions
- Logistics
- Nuclear Security Regime Overview

2

Introductions

- Workshop Director
- NNSA Representative
- Instructors

3

Introduction of Workshop Participants

- Please introduce yourself to the class
  - Name
  - Organization and job
  - Nuclear security experience
  - What you expect to get from this workshop

4

Workshop Schedule

- Day 1
  - Introduction
  - Nuclear Security Regime
- Day 2
  - Physical Protection Systems
- Day 3
  - Transportation Security
  - Physical Protection Decisions to Be Made
  - Next Steps in Collaboration
  - Closing

5

Process of the Workshop

- This is an overview course to provide an awareness of the roles and elements of a Physical Protection Program within a Nuclear Security Regime
- Opportunities for further collaboration on developing or enhancing a nuclear security program will be discussed

6

Workshop Objectives

- Define the legal and regulatory frameworks needed to support Physical Protection
- Identify the functions and elements of a Physical Protection Program
- Recognize the decisions that need to be made to implement Physical Protection Systems

7

Logistics

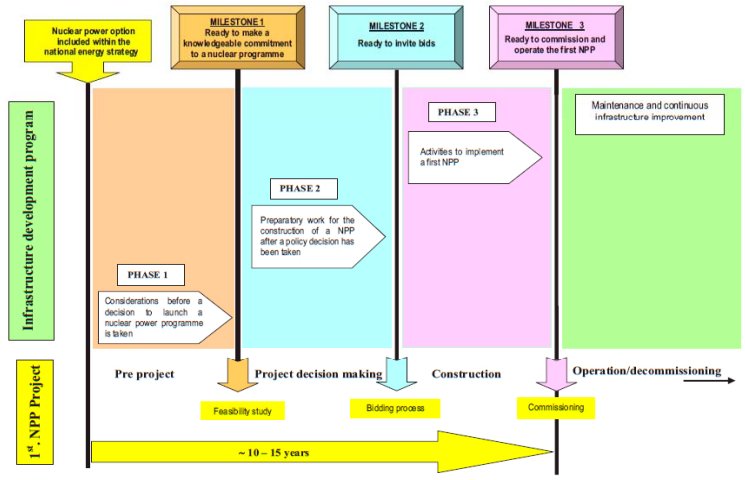
- Breaks
- Exits
- Any questions before we begin?

8

Nuclear Security Overview

9

Infrastructure Milestone Process



Nuclear Power IAEA Nuclear Energy Series No. NG-G-3.1 (Figure extracted from publication)

10

Infrastructure Issues and Milestones

- **19** Infrastructure Issues associated Infrastructure Development
- **3** milestones associated to each Infrastructure Issue

TABLE 1. INFRASTRUCTURE ISSUES AND MILESTONES

Issues	Milestone 1	Milestone 2	Milestone 3
National position			
Nuclear safety			
Management			
Funding and financing	CONDITIONS	CONDITIONS	CONDITIONS
Legislative framework			
Safeguards			
Regulatory framework			
Radiation protection			
Electrical grid			
Human resources development			
Stakeholder involvement			
Site and supporting facilities			
Environmental protection			
Emergency planning			
Security and physical protection			
[illegible]			
Radioactive waste			
Industrial involvement			
Procurement			

11

Physical Protection Infrastructure Issues and Milestones

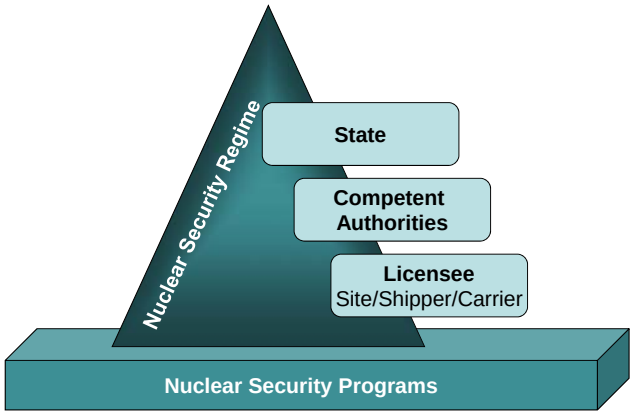
- **3** milestones associated to the Physical Protection Infrastructure Issue
- **Conditions** that would be expected to be achieved by the end of each phase provided in each Milestone

Infrastructure Issue	Milestone 1 Ready to make a knowledgeable commitment to a nuclear program	Milestone 2 Ready to invite bids for the first nuclear power plant	Milestone 3 Ready to commission and operate the first nuclear power plant
3.15 Security and physical protection	•Requirements for security and physical protection acknowledged •Necessary legislation identified	▪Legislation promulgated ▪DBT defined ▪Security requirements defined ▪Sensitive information defined ▪Physical protection by trained on-site security staff provided ▪Local and national law enforcement assistance established ▪Programs for selection/qualification of staff accessing to facilities or sensitive information are in place	•All security conditions established and implemented

Nuclear Power IAEA Nuclear Energy Series No. NG-G-3.1 (Figure extracted from publication)

12

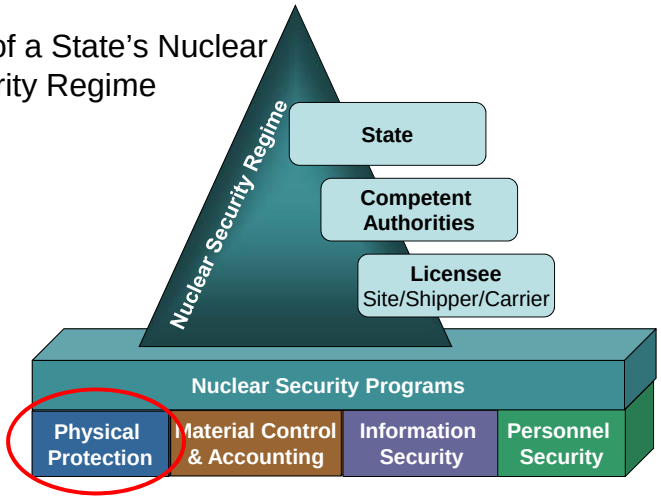
Nuclear Security Regime



13

Physical Protection

Part of a State's Nuclear Security Regime



14

Physical Protection

- PHYSICAL PROTECTION REGIME: A regime that includes the following:
  - the legislative and regulatory framework governing the physical protection of nuclear material, nuclear facilities, and other radioactive materials and associated facilities
  - the institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework
  - facility-level and activity-level physical protection systems
- PHYSICAL PROTECTION PROGRAM: The combination of the physical protection system policies, procedures, and physical protection systems
- PHYSICAL PROTECTION SYSTEM: An integrated set of physical protection measures intended to prevent the completion of a malicious act.

15

Nuclear and Radioactive Material

Benefits

- **Generation of high amounts of carbon-free electrical energy**
- **Medical and industrial uses**
- **Food safety**

Risks

- **Accidents**
- **Target for attack**
- **Radioactive waste**
- **Sabotage**

16

Significant Potential Risks Associated with Nuclear Materials

- Theft
  - Material for an improvised nuclear device
  - Material for a radiation dispersion device
- Sabotage
  - Loss of functionality
  - Dispersion of radioactive material

17

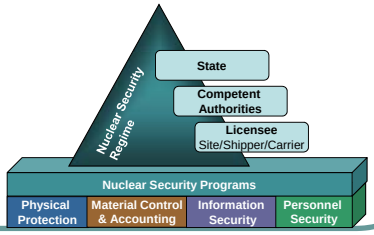
Outline for this Course

- NNSA International Protection Program
- Legal Framework
- Regulatory Framework
- Overview of Nuclear Security Program
- Overview of Physical Protection System (PPS)
  - Requirements Definition, Design Basis Threat, and Targets
  - Characterization and Siting Impacts
  - Elements of PPS Design Detection, Delay, and Response
  - Physical Protection Systems Evaluation
- Transportation Security
- Decisions to be Made
- Next Steps in Collaboration

18

Summary

- Nuclear and other radioactive materials can provide great benefit, but they can also generate significant risks
- **PHYSICAL PROTECTION SYSTEM:** An integrated set of *physical protection measures* intended to prevent the completion of a *malicious act*



19

Conclusion

Questions before we continue?

20

Infrastructure Development: Initiating a Physical Protection Program

Module 2:

NNSA International Physical Protection Program

1

Module Objectives

After completing this module, you should be able to do the following:

- Define Physical Protection Program Scope
- Discuss Physical Protection Program Activity Areas
  - Site Assessments
  - Technical Guidance
  - Professional Training
  - Bilateral Collaboration
- Identify Physical Protection Program Management Tools

2

Need for Physical Protection and IPP Role

- The need to protect nuclear material and facilities globally is imperative; terrorists have demonstrated their willingness to inflict mass causalities and have announced their intention to acquire nuclear material.
- The NNSA Office of Nuclear Safeguards and Security works to ensure physical protection of nuclear material and facilities by
  - Bilateral physical protection visits
  - Development and support of international nuclear security policy and guidance
  - Training of personnel responsible for protecting nuclear material
  - Bilateral technical collaboration

3

Cooperation with Other U.S. Organizations and the IAEA

- Collaborate on physical protection with
  - National Nuclear Security Administration's Office of Defense Nuclear Security, Office of Global Threat Reduction, and the Office of International Material Protection & Cooperation
  - Department of Energy's Office of Counter Terrorism
  - Department of Homeland Security
  - Department of State
  - Nuclear Regulatory Commission
  - Defense Threat Reduction Agency
  - Sandia (SNL) and other U.S. National Laboratories
  - International Atomic Energy Agency (IAEA)

4

Program Scope

- Physical protection of nuclear material during use, storage, and transport
- U.S.-obligated nuclear material in countries with bilateral agreements
- IAEA Office of Nuclear Security and Member States
- Bilateral collaboration with non-weapon states
  - Excluding implementation of upgrades

5

Site Assessments

- Countries with U.S.-obligated nuclear material (approx. 50)
- Physical protection obligation specified in "123" Agreement
- Based on international norm of IAEA INFCIRC/225
  - Compliance required for exports
- Physical protection exchange visits
- Assessment is not an inspection

Bilateral Physical Protection Visits to 46 Countries

Countries Visited

7

Technical Guidance
(NA243/SNL support)

- IAEA Nuclear Security Series
  - Fundamentals
  - Recommendations
  - Implementing Guides
  - Technical Guidance
- Process
  - Document Preparation
  - Consultancy Meetings
  - Technical Meetings

8

IPP Assistance with NSS Publications

- Protection against an Insider Threat
- Nuclear Security Culture
- Development of Design Basis Threat
- Identification of Vital Areas
- Protection against Sabotage
- Nuclear Security Fundamentals
- Protection of Nuclear Material and Facilities (INFCIRC/225/Rev.5) in development

9

Professional Training

- Original U.S. commitment in Nuclear Nonproliferation Act of 1978
- International Training Course (ITC) on Physical Protection of Nuclear Facilities and Materials
  - Over 600 participants from 60 countries
  - Lectures, subgroup exercises, field activities, and final comprehensive exercise using hypothetical facility
  - Taught by SNL in Albuquerque, 3 weeks, in English
  - ITC-21 completed in May 2009

10

Professional Training (cont.)

- IAEA courses developed and presented via NA-241/SNL process
  - RTC PP of NM and NF
  - RTC Security of RR
  - RTC Foundations of PP
  - Design Basis Threat
  - Protection against Sabotage
  - Vital Area Identification
  - Insider Threat
  - Nuclear Security Culture

11

Bilateral Collaboration

- Based on U.S. nuclear material security interests
- Twin objectives
  - Enhance international nuclear security
  - U.S. intellectual gain
- Recent and current partners
  - Japan
  - Republic of Korea
  - France
  - Brazil
  - Argentina

12

Summary

- Program scope includes physical protection of nuclear material, U.S.-obligated nuclear material, IAEA Office of Nuclear Security and member states, bilateral collaboration
- Program activity areas include
  - Site Assessments
  - Technical Guidance
  - Professional Training
  - Bilateral Collaboration

13

Conclusion

Questions before we continue?

14

This page intentionally left blank.

Infrastructure Development: Initiating a Physical Protection Program

Module 3:
Legal Framework

1

Module Objectives

After completing this module, you should be able to do the following:

- Be aware of the legal responsibilities of the State for the security of nuclear and other radioactive material
- Recognize decisions that need to be made at the State level

2

International Legal Instruments Physical Protection

- Nuclear Materials
  - Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment
  - The Physical Protection of Nuclear Materials and Nuclear Facilities, INFCIRC/225/Rev.4 (corrected)
- Other Radioactive Materials
  - Code of Conduct on the Safety and Security of Radioactive Sources
  - Guidance on the Import and Export of Radioactive Sources
- Convention on the Suppression of Acts of Nuclear Terrorism
- UN Security Council resolutions 1373 (2001) and 1540 (2004)
- Safeguards agreements and their additional protocols

3

Convention on the Physical Protection of Nuclear Material (CPPNM)

- Defines what is “nuclear material”
  - plutonium except that with isotopic concentration exceeding 80% in plutonium-238; uranium-233; uranium enriched in the isotope 235 or 233; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore-residue
- Identifies State’s Responsibilities
  - Each State Party shall take appropriate steps within the framework of its national law and consistent with international law to ensure nuclear material is protected at the levels commensurate with the type of material

4

CPPNM – Legal Responsibilities

- Controlled import/export of nuclear materials
- Security of nuclear materials while in transit within and across the State, by land, water, and air
- Designation of central or competent authority for the physical protection of nuclear material and coordinating recovery and response operations
- Protection of the confidentiality of information
- Criminal penalties

5

CPPNM – Criminal Penalties

The intentional commission of:

- an act without lawful authority which constitutes the receipt, possession, use, transfer, alteration, disposal or dispersal of nuclear material and which causes or is likely to cause death or serious injury to any person or substantial damage to property;
- a theft or robbery of nuclear material;
- an embezzlement or fraudulent obtaining of nuclear material;
- an act constituting a demand for nuclear material by threat or use of force or by any other form of intimidation;
- a threat:
  - to use nuclear material to cause death or serious injury to any person or substantial property damage, or
  - to commit an offence in order to compel a natural or legal person, international organization or State to do or to refrain from doing any act;
- an attempt to commit or participate in any offence listed above

6

CPPNM Amendment

- Explicitly includes nuclear material and *nuclear facilities*
- Added sabotage considerations
- The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State Party rests entirely with that State.
  - Establish and maintain a legislative and regulatory framework to govern physical protection;
  - Establish or designate a competent authority or authorities responsible for the implementation of the legislative and regulatory framework; and
  - Take other appropriate measures necessary for the physical protection of nuclear material and nuclear facilities.
- Adds the 12 Fundamental Principles for Physical Protection of nuclear material and nuclear facilities

7

12 Physical Protection Fundamental Principles

1. Responsibility of the State
2. Responsibilities during international transport
3. Legislative and regulatory framework
4. Competent authority
5. Responsibility of the license holders
6. Security culture
7. Threat
8. Graded approach
9. Defense-in-depth
10. Quality assurance
11. Contingency plans
12. Confidentiality

From the International Atomic Energy Agency (GOV/2001/41)

8

CPPNM Amendment (continued)

- Each State Party shall establish, implement and maintain an appropriate physical protection regime applicable to nuclear material and nuclear facilities under its jurisdiction, with the aim of:
  - (a) protecting against theft and other unlawful taking of nuclear material in use, storage and transport;
  - (b) ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material; when the material is located outside its territory, that State Party shall act in accordance with article 5;
  - (c) protecting nuclear material and nuclear facilities against sabotage; and
  - (d) mitigating or minimizing the radiological consequences of sabotage

9

CPPNM – Extended Criminal Penalties

- Add the environment to impacts of malicious acts
- Added robbery, embezzlement, and fraudulent obtaining of nuclear material
- Added an act which constitutes the carrying, sending, or moving of nuclear material into or out
- of a State without lawful authority;
- Extended the range of criminal actions to
  - Demanding nuclear material by threat or use of force or by any other form of intimidation;
  - Threatening to use nuclear material to cause death or serious injury to any person or substantial damage to property or to the environment
  - Planning, attempt, threat of, commission, participation in malicious acts using nuclear material or against nuclear facilities

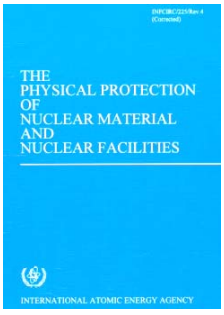
10

Is your country a signatory to CPPNM?
To its Amendment?

11

INFCIRC 225/Rev 5

- **Objectives of a State's Physical Protection Regime**
- **Elements of a State's Physical Protection Regime for Nuclear Material and Nuclear Facilities**
- **Requirements for Measures Against**
  - **Unauthorized Removal of Nuclear Material in Use and Storage**
  - **Sabotage of Nuclear Facilities and Nuclear Material in Use and Storage**
  - **Unauthorized Removal and Sabotage of Nuclear Material During Transport**



12

INFCIRC 225/Rev 5 – Legislative Framework Requirements

A State should

- Take appropriate measures within the framework of its national law to establish and ensure the proper implementation of the State's physical protection regime.
- Define requirements for the physical protection of nuclear material in use, in storage, and during transport, and for nuclear facilities depending on the associated consequences of either unauthorized removal of nuclear material or sabotage.
- Provide for the regulation of physical protection and include a licensing requirement. The regulations should be applicable to all such materials and facilities regardless of whether under State or private ownership.
- License activities only when they comply with its physical protection regulations.
- Ensure that evaluations also include exercises to test the integrated system, including the training and readiness of guards and/or response forces.
- Determine the trustworthiness policy
- Include enforcement of physical protection regulations as a part of a State's physical protection regime.
- Provide sanctions against the unauthorized removal of nuclear material and against sabotage

13

Guidance for Other Radioactive Materials

- Code of Conduct on the Safety and Security of Radioactive Sources
- Guidance on the Import and Export of Radioactive Sources

Countries that have expressed agreement with the Codes

14

Other Governing Documents

- Convention on the Suppression of Acts of Nuclear Terrorism
- Safeguards agreements and the Additional protocol
- UN Security Council resolutions 1373 (2001) and 1540 (2004)

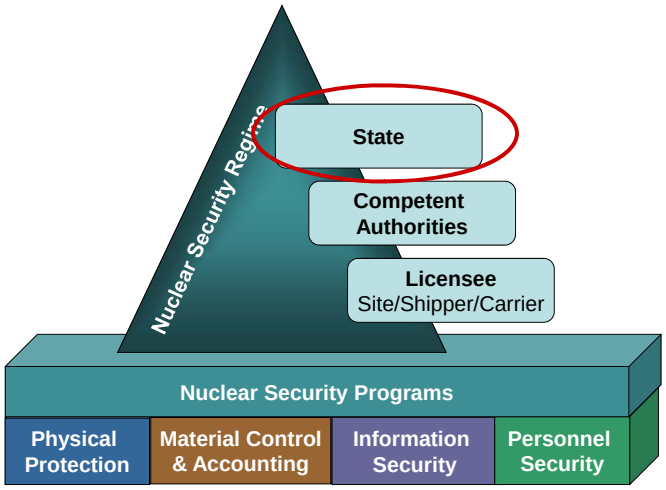
15

Other Guidance Documents

- Technical and Functional Specifications for Border Monitoring Equipment
- Nuclear Forensics Support
- Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators
- Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage
- Identification of Radioactive Sources and Devices
- Combating Illicit Trafficking in Nuclear and other Radioactive Material
- Nuclear Security Culture
- Preventive and Protective Measures against Insider Threats
- Security in the Transport of Radioactive Material
- Development, Use and Maintenance of the Design Basis Threat
- Security of Radioactive Sources
- Educational Programme in Nuclear Security

16

Nuclear Security Regime



17

State Responsibilities Relating to Physical Protection

- Establish legal basis for regulations
- Designate competent authority(s)
- Establish nuclear material accountability and control
- Conduct and maintain an intelligence-based threat assessment
- License only facilities and carriers/shippers who meet physical protection objectives
- Provide security transport of nuclear and other radioactive materials
- Designate appropriate response forces

18

Legal Issues

- **Most complex and difficult**
- **Legal issues include:**
  - Security liability (provide reasonable security)
  - Failure to protect (negligence liability)
  - Overreaction (excessive force, invasion of privacy, guard instructions and training)
  - Labor/employment issues (labor unions, work practices)

19

19

Decisions to Be Made

- Full participation in international agreements
- Government agency(s) will be responsible for the physical protection of nuclear and radioactive materials
- Nuclear and radioactive materials permitted in your country
- Who will conduct an intelligence-based threat assessment and how will decisions be made based on this threat assessment
- Licensing process and evaluation of continued compliance
- Level of personnel trustworthiness requirements
- Classification and associated protection of information and nuclear/radioactive materials
- Mechanisms for security transport of nuclear and other radioactive materials
- Response force responsibility
- Agency for working with legislative body

20

Summary

- The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State
- The legal framework provides the authorities and penalties associated with nuclear and other radioactive materials
- There are many decisions associated with establishing a nuclear security regime and physical protection program

21

Conclusion

Questions before we continue?

22

This page intentionally left blank.

Infrastructure Development: Initiating a Physical Protection Program

Module 4:
Regulatory Framework

1

Module Objectives

After completing this module, you should be able to do the following:

- Recognize the requirements for a regulatory framework
- Identify a regulatory approach for a nuclear security program
- Recognize the considerations for a nuclear security program

2

Physical Protection Infrastructure Issues and Milestones

- **3** milestones associated to the Physical Protection Infrastructure Issue
- **Conditions** that would be expected to be achieved by the end of each phase provided in each Milestone

Infrastructure Issue	Milestone 1 Ready to make a knowledgeable commitment to a nuclear program	Milestone 2 Ready to invite bids for the first nuclear power plant	Milestone 3 Ready to commission and operate the first nuclear power plant
3.15 Security and physical protection	•Requirements for security and physical protection acknowledged •Necessary legislation identified	•Legislation promulgated •DBT defined •Security requirements defined •Sensitive information defined •Physical protection by trained on-site security staff provided •Local and national law enforcement assistance established •Programs for selection/qualification of staff accessing to facilities or sensitive information are in place	•All security conditions established and implemented

Nuclear Power IAEA Nuclear Energy Series No. NG-G-3.1 (Figure extracted from publication)

3

Evaluation Status of Milestone 1

15. Security[a]	Phase 1
Conditions	Basis for evaluation
15.1. Requirements for security and physical protection acknowledged.	• Establishment of an committee forf nuclear security-related policy making, interagency coordination and planning activities associated with security and physical protection. Clear definition of its role, structure, responsibilities and reporting requirements. • Evidence of suitable qualifications and experience of the members. • A plan to implement a division/office responsible for the management of security and physical protection arrangements, including an organizational chart and a description of its function. • A plan to hire or contract with SQEP (suitably qualified and experienced personnel) experts and organizations to assist in security and vulnerability analysis as well as risk assessments of malicious acts to nuclear power plants, nuclear and other radioactive material and its transportation. • Government awareness of the risk of malicious acts and possible radiological, political, economical and social consequences. Evidence of intelligence service technical reports on the analysis of incidents occurring at nuclear facilities in the world. • Government awareness of international guidelines on security.[b] • Plan to train relevant staff including police and armed forces. • Programme to develop strong security culture during phase 2.
15.2. Necessary regulation identified.	• Plan to develop national legislation providing a basis for regulation of security and physical protection arrangements regarding nuclear facilities, nuclear and other radioactive material, its transportation and storage, including provisions for licensing, inspection, and sanctions. • Plan to develop a regulatory function in the area of security and physical protection, including physical protection requirements, information confidentiality, security staff recruitment, security culture and other components. • A set of requirements such as those in IAEA Nuclear Security Series. • A plan, including allocation of adequate resources, for the production of regulatory documents. • Clear identification of a head organization that will manage a national DBT (design basis threat) development. • A plan to collect documents, information, data from investigations and other source data on illegal, malicious, criminal and other acts, in order to carry out a risk assessment and modelling scenarios of illegal activities. • Evidence that external and other threats have been considered for the selected nuclear power plant sites in order to minimize the risk of malicious acts.
15.3. Effective security protection for existing uses of radiation sources in place	• Report of an audit/review of the existing protection against international requirements with a resulting action plan which is being met.

[a] Note that security considerations include physical protection and adequate consideration of safety needs and vice versa.
[b] See the publications in the IAEA Nuclear Security Series.

4

Evaluation Status of Milestone 2

15. Security [a]	Phase 2
Conditions	**Basis for evaluation**
15.1. Legislation promulgated.	• Arrangements and draft of agreements covering protocols and programmes for local and national law enforcement assistance.
15.2. DBT defined.	• The design basis threat defined and outline of security requirements included in the BIS.
15.3. Security requirements defined.	• Security requirements and desirable features planned for the site. • Evidence that best practise for security at the nuclear power plant is understood.
15.4. Sensitive information defined.	• Procedures for the definition and protection of sensitive information. Penalties for violation available and supported by legislation.
15.5. Physical protection by trained on-site security staff provided.	• Security requirements during construction defined, including on-site civil security personnel and a policy on whether armed, and a plan for their implementation.
15.6. Programmes for selection/qualifications of staff with access to facilities are in place.	• Adequate screening programmes for recruitment and selection of personnel with access to facilities and classified documentation.
15.7. Security culture promulgated.	• Evidence of the promulgation of a security culture, recognizing the importance of nuclear material, within all key organizations involved in the nuclear power programme.

[a] Note that security considerations include physical protection and also need to include adequate consideration of safety needs and vice versa.

5

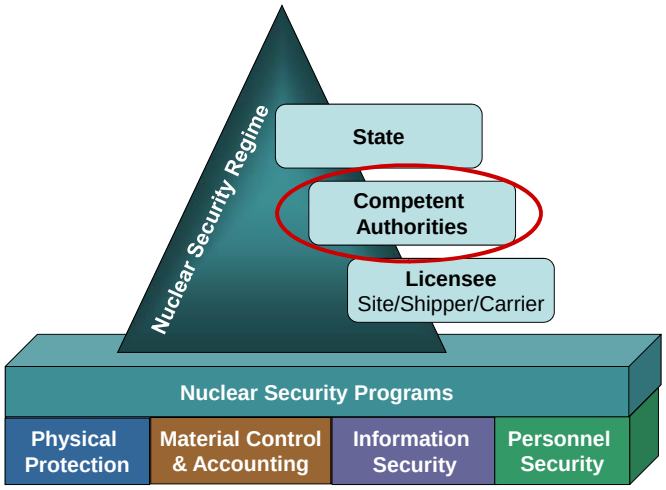
Four Physical Protection Objectives
INFCIRC/225/Rev 5

- Protect against unauthorized removal of nuclear material in use and storage, and during transport;
- Ensure the implementation of rapid and comprehensive measures by the State to locate and recover missing or stolen nuclear material;
- Protect against sabotage of nuclear facilities and sabotage of nuclear material in use and storage and during transport; and
- Mitigate or minimize the radiological consequences of sabotage.

IAEA document GC(45)/INF/14, Sept 2001

6

Nuclear Security Regime



7

Nuclear Security Regulatory Framework

- Competent Authority(s)
- Regulations
- Guides

8

Competent Authority(s)

- State agency(s) responsible under national law that have the legally delegated or invested authority, capacity, or power to license and regulate:
  - nuclear materials and facilities
  - other radioactive materials and facilities that use them
  - shippers, carriers, and receivers of nuclear and other radioactive materials

9

Regulations

- Provide architecture for more detailed conditions and requirements
- Mandatory
- Based on internationally recognized standards and guidelines
- Serve as a basis for licensing and inspections

10

Guides

- Guidance on how to comply with regulations
- Non-mandatory

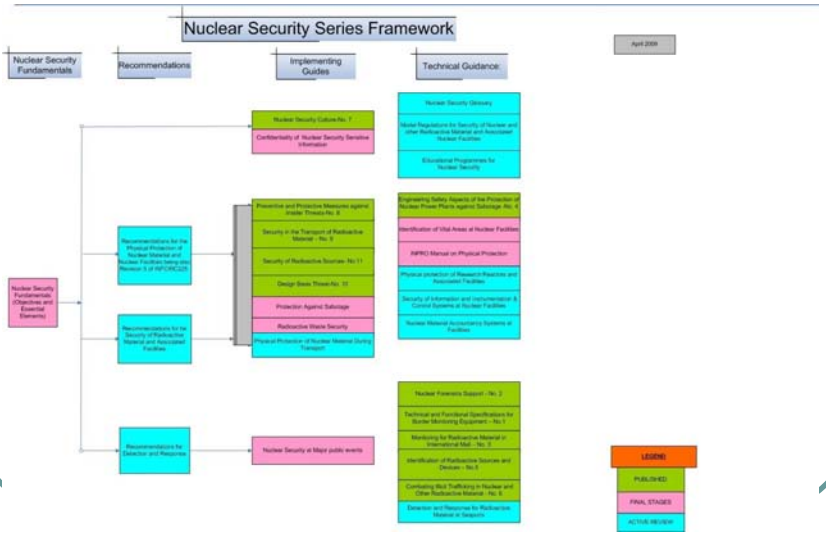
11

Physical Protection Documents

- Major Documents
  - Physical Protection Fundamentals GOV/2001/41
  - The Physical Protection of Nuclear Material and Nuclear Facilities INFCIRC/225/Rev. 4 (corrected)
- Supporting Documents
  - TECDOC-967 (Rev. 1)
  - TECDOC 1276: Handbook

12

Nuclear Security Series



13

IAEA Nuclear Security Series – Implementing Guides

- Nuclear Security Culture
- Preventive and Protective Measures against Insider Threats
- Security in the Transport of Radioactive Material
- Development, Use and Maintenance of the Design Basis Threat
- Security of Radioactive Sources

14

Basic Steps for Developing a Regulatory Framework

- Define undesired consequences
- Establish graded Security Levels with corresponding protection goals
- Correlate nuclear and other radioactive materials to Security Levels
- Select and implement a regulatory approach

15

Undesired Consequences

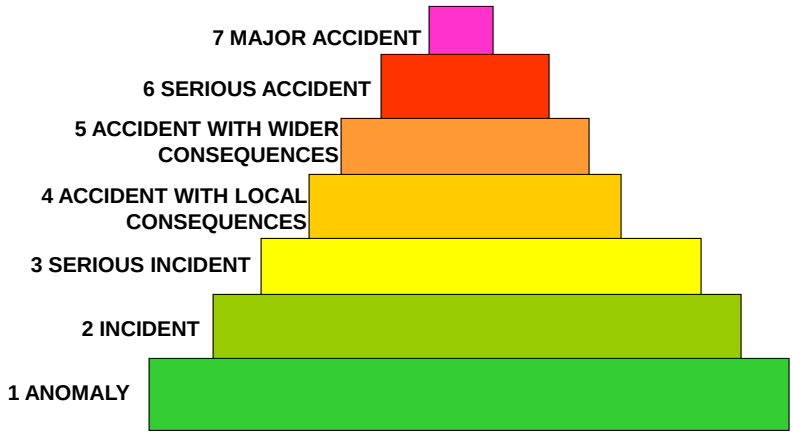
Economic Loss

Environmental Contamination

Political Upheaval/ Loss of Public Confidence

16

Nuclear and Radiological Event Scale



www.iaea.org/Publications/Factsheets/English/ines.pdf

17

INFCIRC/225/Rev.4 (corrected)

- Provides a set of recommendations on requirements for the physical protection of nuclear material in use and storage and during transport and of nuclear facilities.
- Provides a categorization of the different types of nuclear material.
- Links protection levels to categories of material.
- Currently under revision to address the current threat environment and ensure conformance to CPPNM.

18

Nuclear and Radiological Event Scale

EXAMPLES OF EVENTS AT NUCLEAR FACILITIES

	People and Environment	Radiological Barriers and Control	Defence-in-Depth
7	*Chernobyl, 1986* — Widespread health and environmental effects. External release of a significant fraction of reactor core inventory.		
6	*Kyshtym, Russia, 1957* — Significant release of radioactive material to the environment from explosion of a high activity waste tank.		
5	*Windscale Pile, UK, 1957* — Release of radioactive material to the environment following a fire in a reactor core.	*Three Mile Island, USA, 1979* — Severe damage to the reactor core.	
4	*Tokaimura, Japan, 1999* — Fatal overexposures of workers following a criticality event at a nuclear facility.	*Saint Laurent des Eaux, France, 1980* — Melting of one channel of fuel in the reactor with no release outside the site.	
3	*No example available*	*Sellafield, UK, 2005* — Release of large quantity of radioactive material, contained within the installation.	*Vandellos, Spain, 1989* — Near accident caused by fire resulting in loss of safety systems at the nuclear power station.
2	*Atucha, Argentina, 2005* — Overexposure of a worker at a power reactor exceeding the annual limit.	*Cadarache, France, 1993* — Spread of contamination to an area not expected by design.	*Forsmark, Sweden, 2006* — Degraded safety functions for common cause failure in the emergency power supply system at nuclear power plant.
1			Breach of operating limits at a nuclear facility.

19

Nuclear and Radiological Event Scale

EXAMPLES OF EVENTS INVOLVING RADIATION SOURCES AND TRANSPORT

	People and Environment	Defence-in-Depth
7		
6		
5	*Goiânia, Brazil, 1987* — Four people died and six received doses of a few Gy from an abandoned and ruptured highly radioactive Cs-137 source.	
4	*Fleurus, Belgium, 2006* — Severe health effects for a worker at a commercial irradiation facility as a result of high doses of radiation.	
3	*Yanango, Peru, 1999* — Incident with radiography source resulting in severe radiation burns.	*Ikitelli, Turkey, 1999* — Loss of a highly radioactive Co-60 source.
2	*USA, 2005* — Overexposure of a radiographer exceeding the annual limit for radiation workers.	*France, 1995* — Failure of access control systems at accelerator facility.
1		Theft of a moisture-density gauge.

20

Graded Protection Approaches

- The application of physical protection measures proportional to the potential consequences of a malicious act.
- Target categorization tables provide a means to apply graded levels of protection.
- Different graded approaches may be considered:
  - Grade system effectiveness – all systems use the same Design Basis Threat (DBT) but require less effective systems for lower consequence targets
  - Grade the threat for targets – all targets/systems meet the same level of performance, but the lower-consequence targets use a lower-level threat
  - Grade both system effectiveness and threat for targets

21

IAEA Categorization of Nuclear Material

Material	Form	Category I	Category II	Category III[c]
1. Plutonium[a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235	Unirradiated[b] – uranium enriched to 20% ^{235}U or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15 g
	– uranium enriched to 10% ^{235}U but less than 20% ^{235}U		10 kg or more	Less than 10 kg but more than 1 kg
	– uranium enriched above natural, but less than 10% ^{235}U			10 kg or more
3. Uranium-233	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated Fuel (The categorization of irradiated fuel in the table is based on international *transport* considerations. The State may assign a different category for domestic use, storage, and *transport* taking all relevant factors into account.)			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[cde]	

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/hr
[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.
[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.
[e] Other fuel which by virtue of its original material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/hr (100rad/hr) at one meter unshielded.

22

Example of Security Levels Based on Nuclear Materials

- Category I – Strategic Special Nuclear Material
- Category II – Special Nuclear Material of moderate strategic significance
- Category III – Special Nuclear Material of low strategic significance

Goal: To establish conditions that minimize the possibility of *sabotage* and/or *unauthorized removal* of nuclear material

23

Categorization Table for Radioactive Materials

Category	Source	A/D	Security level
1	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	A/D ≥ 1000	A
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D ≥ 10	B
3	Fixed industrial gauges that incorporate high activity sources Well logging gauges	10 > A/D ≥ 1	C
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D ≥ 0.01	Apply measures as described in the Basic Safety Standards [5]
5	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt	

24

Example of Security Levels for Radioactive Sources

- The IAEA recommends the following Security Levels and associated goals for radioactive materials:
  - Security Level A: **prevent** unauthorized removal of a source (timely detection and response)
  - Security Level B: **minimize the likelihood** of unauthorized removal of a source (immediate detection of the unauthorized removal, but not requiring a response to interrupt the act)
  - Security Level C: **reduce the likelihood** of unauthorized removal of a source

25

Threat - Design Basis Threat (DBT)

- State regulatory tool used for planning, designing, and evaluating a PPS
- Covers both theft and sabotage
- Describes attributes and characteristics of potential adversaries
- Not an explicit description of the expected adversary:
  - Provides basis for State-wide consistency
  - May change as events occur
  - Supports prudent PPS within cost constraints

26

Regulatory Approach

1. Prescriptive
   - Three-meter-high fence
   - Sensors in storage area
2. Performance-based
   - Have performance effectiveness greater than *yy*
3. Combination of the two
   - Have volumetric sensor with minimum probability of detection *yy*

27

Advantages and Disadvantages

Design Approach	Advantages	Disadvantages
Prescriptive Criteria	Easy to apply, easy to measure	No assurance of desired performance
Performance Criteria	Identifies effectiveness	More difficult to apply, requires expertise

28

Combination Approach

- Use both prescriptive and performance requirements
- Prescriptive requirements where quantification is difficult
- Performance requirements should be in as many areas as feasible
- The combination leads to improved cost-effectiveness

29

Approach Comparison

Approach	System Goal	Effectiveness Measures
Prescriptive Criteria	Include required features (Example: three perimeter sensors required)	Number of features present or feature performance
Performance Criteria	Meet PPS objectives (Example: perimeter system to detect intruder)	Overall system performance
Combined Feature and Performance	Apply feature and performance criteria as appropriate to meet PPS objectives	Overall performance or feature presence

30

Nuclear Security Regulatory Architecture

1. Licensing
2. Definitions
   a) Information and Material Classification System
   b) Design Basis Threat
3. Requirements for each type of material
   a) Personnel Trustworthiness
   b) Physical Protection Systems
   c) Response Force
   d) Information Security
   e) Material Control and Accounting
   f) Import/Export
4. Considerations
   a) Security Culture
   b) Defense-in-Depth
   c) Graded Approach
   d) Contingency Planning
   e) Emergency Preparedness/Response
   f) Quality Assurance

31

Considerations

a) Security Culture
b) Defense-in-Depth
c) Contingency Planning
d) Emergency Preparedness
e) Quality Assurance

32

Security Culture

- Nuclear Security Culture: all organizations involved in implementing physical protection should
  - Give due priority to the security culture
  - Provide for its development and maintenance
  - Ensure its effective implementation in the entire regime
- Radioactive Sources Security Culture
  - Every State should, in order to protect individuals, society, and the environment, take the appropriate measures to ensure … the promotion of safety culture and of security culture with respect to radioactive sources.

33

Defense-in-Depth

- The State's requirements for physical protection should reflect a concept of several layers and methods of protection that have to be overcome or circumvented by an adversary in order to achieve adversary objectives:
  - Structural
  - Technical
  - Personnel
  - Organizational

34

Contingency Plans

- Emergency plans to respond to the following:
  - Unauthorized removal of nuclear material
  - Sabotage of nuclear facilities or nuclear material
  - Attempts at either

35

Emergency Preparedness/Response

- Compensatory measures for
  - Failure of physical protection equipment
  - Reduced security personnel status
  - Medical emergencies or fire

36

Quality Assurance

- Policy and program established to provide confidence that specified requirements for all activities important to physical protection are satisfied:
  - Inspections
  - Performance Testing
  - Change Management

37

Decisions to be Made

- Develop a regulatory approach
  - Prescriptive or Performance-based or Combination
- Regulatory framework covering:
  - Licensing
  - Definitions
  - Requirements
  - Considerations
- Graded approach framework

38

Summary

- Requirements for a regulatory framework
- Identify a regulatory approach for a nuclear security program
- Recognize the considerations for a nuclear security program

39

Conclusion

Questions before we continue?

40

Infrastructure Development: Initiating a Physical Protection Program

Module 5:

Overview of Nuclear Security Programs and Their Relationship to Physical Protection

1

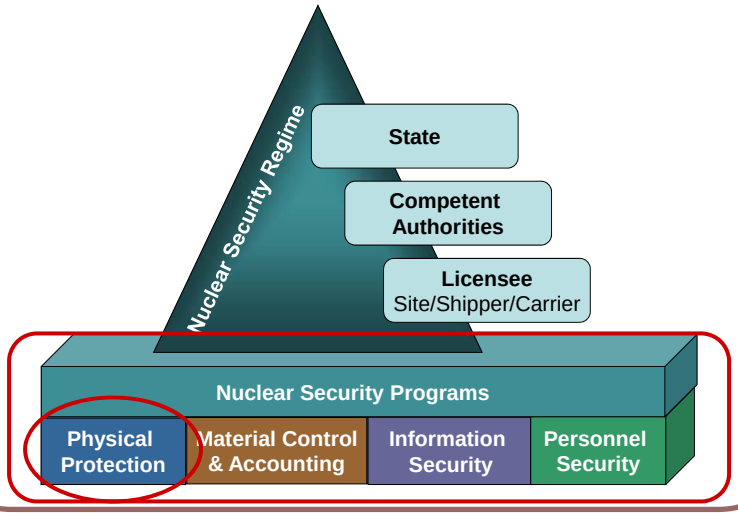
Module Objectives

After completing this module you should be able to do the following:

- Describe the four programs that support a Nuclear Security Program
- Describe a Physical Protection Program
- Describe the relationship between Material Control and Accounting, Information Security, Personnel Security and Physical Protection
- Describe the decisions that must be made to support Physical Protection

2

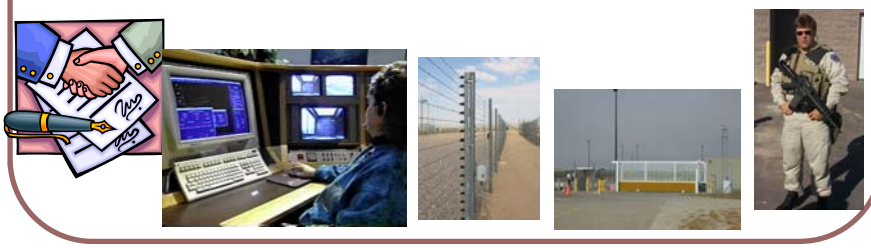
Nuclear Security Reference Model



3

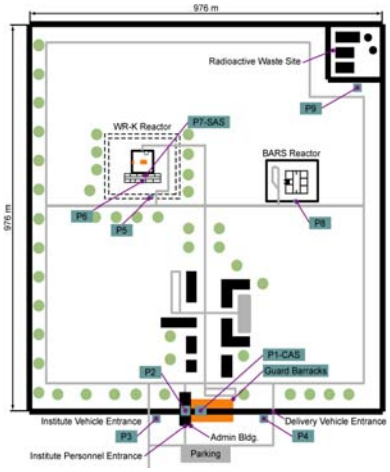
Physical Protection Program

A physical protection program, is the integration of people, procedures, and equipment used to protect assets or facilities against theft, sabotage, or other malicious human attacks.



4

Fixed Site Physical Protection System



5

Transportation Physical Protection System

- Material movement within a site
- Material movement to and from a site

Spent-Fuel Cask on Rail Car

6

Design and Evaluation Approaches

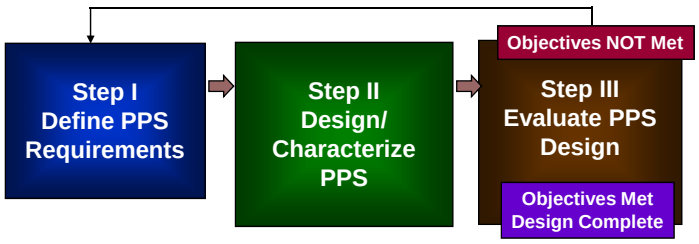
Approach	Requirement	Metric
Expert	Satisfy expert	Opinion
Prescriptive	Include required features	Presence of features
Component Criteria	Include required features that meet specific standards	Presence of feature and performance standard
Performance	Prevent theft or sabotage of nuclear material	System effectiveness

INFCIRC/225/Rev. 4 – "The State should define requirements for the PPS"

7

A System Engineering Process

- Three interdependent steps required:



Repeat process until risk is acceptable (iterative process)

8

Define Requirements

- Understand the threat
- Identify the assets of interest
- Characterize the environment
- Existing facility or facility design
  - Operational states
  - Employee populations
  - Existing physical protection
  - Terrain, climate, weather, etc.

Step I
Define PPS Requirements

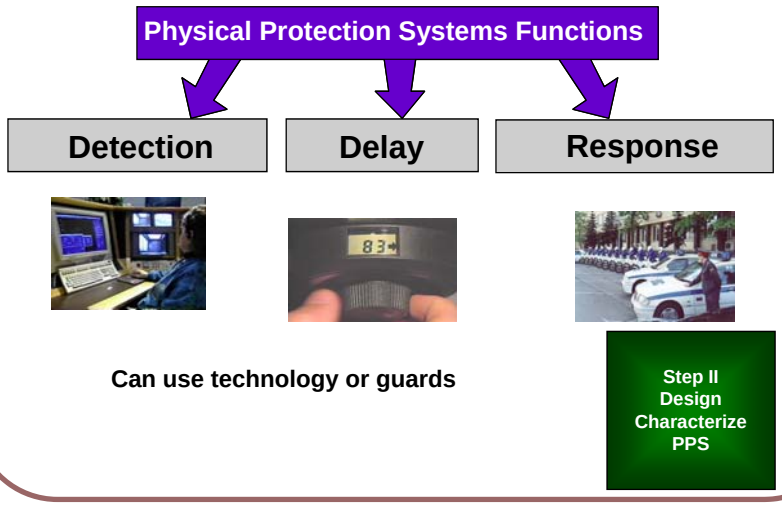
9

Physical Protection Goals

- Deter attack
- Detect attack as it begins and as it progresses
- Increase adversary time to complete task through delay
- Respond to attack in timely and effective manner

10

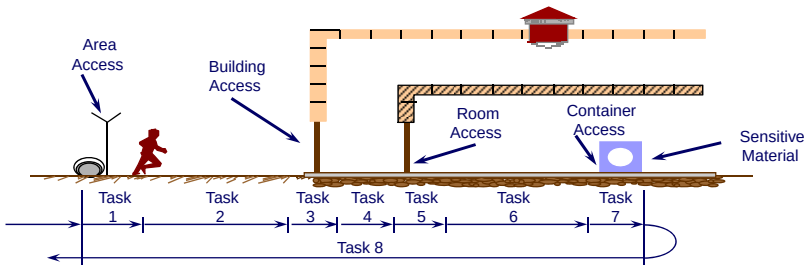
PPS Functions



11

Security Event Sequence Example

For a successful system design, the total time for detection, delay, and response must be less than adversary task time to complete his or her goal



12

General Definition: Security Risk

- **Security Risk** — exposure to the possibility of future harm or loss due to malicious actions of persons or groups of persons
- Security risk is a function of
  - Frequency of loss describing how often do malicious actions take place
  - The consequence–a measure of harm or loss–that will occur if a malicious action takes place
  - The effectiveness of protection and mitigation measures
- The amount of control each licensee has over each function is different

13

Risk Management

- **Risk avoidance** is accomplished by eliminating the source of the risk. For example moving nuclear or radioactive materials out of a building that cannot adequately protect it to a building specifically designed to protect those kinds of materials.
- **Risk reduction** is achieved by taking some actions to lower risk to the community/facility to reduce the severity of the loss. This is the objective of many security programs – to lower risk by implementing at least some security measures.
- **Spreading the risk** can be accomplished by having similar services/ processes/assets at more than one facility site. By separating assets, fewer assets are at risk during any given adversary attack.
- **Risk transfer** is the use of insurance to cover the replacement or other costs incurred as a result of the loss.
- **Risk acceptance** is the recognition that there will always be some residual risk.

14

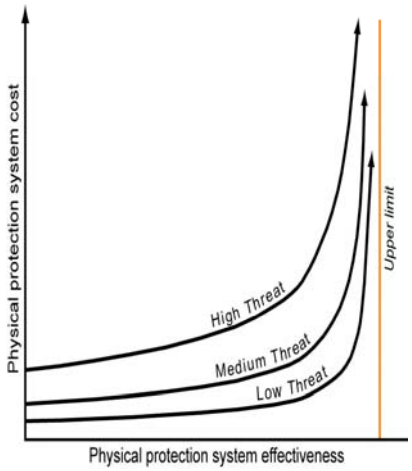
Risk Reduction Strategies

- There are a number of strategies for risk reduction in a State's nuclear program:
  - Consolidation to fewer locations
  - Conversion to less attractive materials
  - Final disposition of excess materials
  - Cost-effective physical protection systems

15

Cost vs. System Effectiveness

The Competent Authority will have to determine how much risk is acceptable vs. the cost of reducing that risk.



16

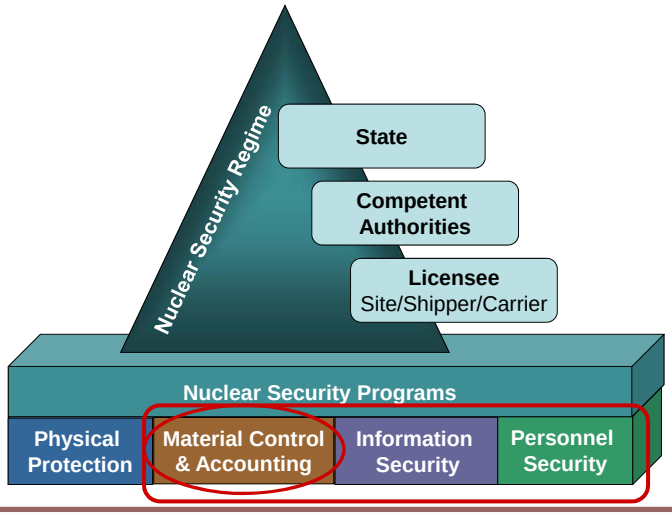
Physical Protection System Summary

A physical protection system is the integration of people, procedures, and equipment used to protect assets or facilities against theft, sabotage, or other malicious human attacks.

- Fixed sites
- Transportation
- Risk component

17

Nuclear Security Reference Model



18

Material Control and Accounting (MC&A)

The MC&A Program functions as a whole to

- provide information on the location and use of strategic nuclear materials,
- provide assurance that they are accessed and processed in a manner appropriate to their strategic significance,
- monitor that the facilities, personnel, and regulations are adequate to deter and detect diversion of nuclear material from its intended purposes, and
- be able to state that 'the nuclear material was adequately accounted for'

19

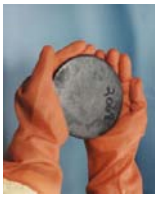
Why is MC&A Important?

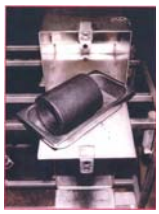
- To provide assurance that nuclear materials are accounted for properly.
- To detect theft or diversion of nuclear materials.
- To act as an integral component of the safeguards system that deters theft or diversion of nuclear materials.
- Or, how do we really know when and how much nuclear material is missing, and how do we deter the potential diverter?

20

Accountable Nuclear Materials

- Those defined in the guidance documents:
  - Fissile Materials (Enriched Uranium, Plutonium, Neptunium, Americium)
  - Source materials used to produce fissile materials (Depleted and Normal Uranium, Thorium)
  - Other materials of special interest, e.g. Tritium, Californium, Curium



21

Other Radioactive Materials of Concern

- **Am-241**
- **Am-241/Be**
- **Cf-252**
- **Cm-244**
- **Co-60**
- **Cs-137**
- **Cd-153**
- **Ir-192**
- **Pm-147**
- **Pu-238**
- **Pu-239/Be**
- **Ra-226**
- **Se-75**
- **Sr-90(Y-90)**
- **Tm-170**
- **Yb-169**

IAEA Code of Conduct Radioactive Materials of Greatest Concern

22

Main Components of MC&A Program

- Accounting
- Measurements and Measurement Control
- Material Control
- Assessments

23

Accounting

- Provide a complete, accurate, and timely record of the nuclear material inventory
- Determine the nuclear material inventory
- Document nuclear material transactions/movements
- Issue periodic reports
- Assist with the detection of material gains or losses, unauthorized data access, and data falsification
- Provide a complete audit trail for all nuclear material from receipt through disposition
- Provide a complete, accurate, and timely record of the nuclear material inventory

Monitoring team taking inventory in storage vault

24

Measurements and Measurement Control

- **Measurements are used to establish and/or confirm the amount of nuclear material present in a specific item, container, or in some cases facility. These measurements may be destructive or nondestructive, but conducted within a measurement control system.**
- **The Measurement Control system is designed to ensure measurement stability, establish measurement uncertainty, and to ensure measurements meet the quality objectives required by the safeguards system.**
- **All of these efforts are ultimately designed to provide confidence in measurement results and assurance that the measurement uncertainties are well known and adequate for their needs**

25

Material Control

- **Controls the location and use of nuclear materials through appropriate systems of containment and surveillance**
- **Ensures that nuclear materials are used, processed, or stored only in areas that have been identified for these purposes.**
- **Provides sealing and containment for materials that are being stored or transported.**
- **Establishes boundaries where nuclear materials can be located, along with controls for these boundaries, and provides controls governing the use of materials within these boundaries.**
- Includes
  - Access requirements for facilities, nuclear information databases, areas within a facility, etc.
  - Covering procedures for handling, processing, inventorying and reporting on nuclear materials
  - Personnel surveillance when working in nuclear material areas
  - Material containment and surveillance systems

It is accomplished with people, procedures, technology.

26

Assessments

- Ensure the integrated MC&A system is capable of detecting and assessing unauthorized removals of nuclear material
- Ensure that detection elements provide sufficient information to correctly assess alarms and to quantify and localize losses
- Monitor and evaluate:
  - Inventory differences
  - Shipper/Receiver differences
  - Anomalies
  - Related statistical/confidence limits
- Routinely evaluate the MC&A system by introducing anomalies to determine if these artificial anomalies are detected
- Assess unauthorized removals of nuclear material

Weighing items in process area

27

Unsuccessful MC&A

What can happen when MC&A isn't effective

- Shutdown of operations
- Undiscovered Diversion/Theft
- Unexplained Loss
- Poor Criticality Safety
- Poor Environmental Stewardship
- Loss of Credibility with citizens, international community, United Nations
- Successful adversarial attacks

28

Impacts to Physical Protection

- Material unaccounted for can result in security events to which the physical protection system must respond
- Material categorizations can determine the level of physical protection required
- Access to material must be controlled through the access control system in a physical protection system

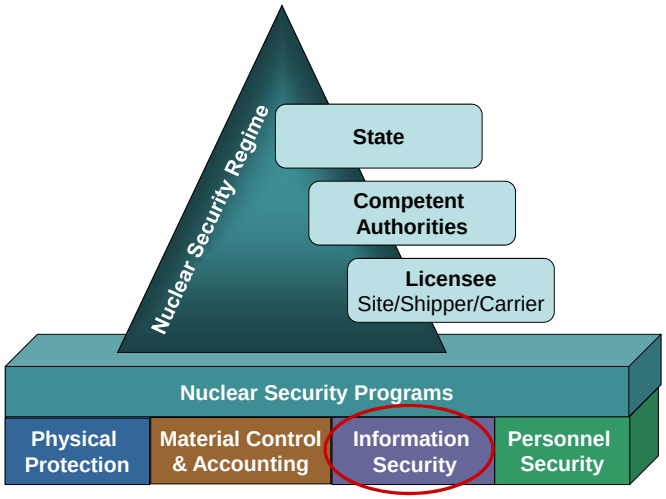
29

Confidentiality

- Requirements for protecting the confidentiality of information (one of the 12 fundamental principles)
- Applicable when unauthorized disclosure could compromise the physical protection of nuclear material and nuclear facilities

30

Nuclear Security Reference Model



31

Information Systems

Systems where information is stored, used, or transmitted

Physical

- Paper-based systems
- Policies, procedures, access control lists

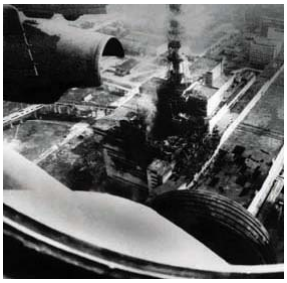
Cyber

- Electronic or network-based systems

32

Threats to information systems have significant consequences

- Theft of classified information or materials
- Loss of services – internal and external
- Contamination of surrounding population



33

Who are the adversaries?

Outsider? Insider?

Cyber Adversary → **Characterized by**

Commitment
- Intensity
- Stealth
- Time

Resources
- Technical Personnel
- Cyber/Kinetic Knowledge
- Access

34

Common Cyber Adversary Tools

- Virus
- Worm
- Denial of Service
- Remote Access Capabilities

35

Information Security Protection Measures

- Administrative Controls
- Password Management
- Technical Controls
- Mitigation/Recovery

36

Administrative Controls

- Training
- Policies and procedures
- Password Management
- Principle of Least Privilege
- Administrative Controls (similar to access control)

Increases the number of "sensors" for unauthorized activity

37

Password Management

Raise your hand if you have a computer password?

38

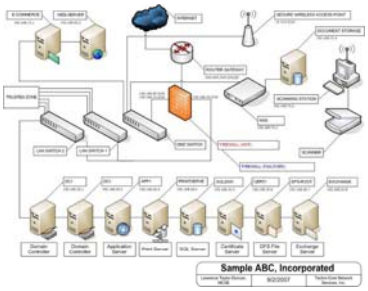
Password Management (cont.)

- Change often
  - Every 6 months or annually
  - Whenever possibly compromised
- Limit number of failed password attempts
- Immediately delete user accounts when personnel terminate employment or contracts are terminated

39

Technical Controls

- Network Design and Configuration Management
- Detection and Logging
- Firewalls
- Routers
- Virus Protection



40

Mitigation/Recovery

- Policies, architectures, frameworks, and accountabilities used to lessen risk by lower its chances of happening or reducing its effect if it does occur
  - Graceful degradation while under attack
  - Survivable functions
  - Network isolation
  - Recovery of systems/data
  - Compensatory measures
- Periodic backups/mirror images made, tested, and protected at the same level as the original, but not at the same location

41

Physical Protection & Information Systems

- Physical Protection of Information Systems
  - Critical assets that must be protected
- Cyber Systems are part of Physical Protection Systems
  - Access controls
  - Sensor and alarm communications

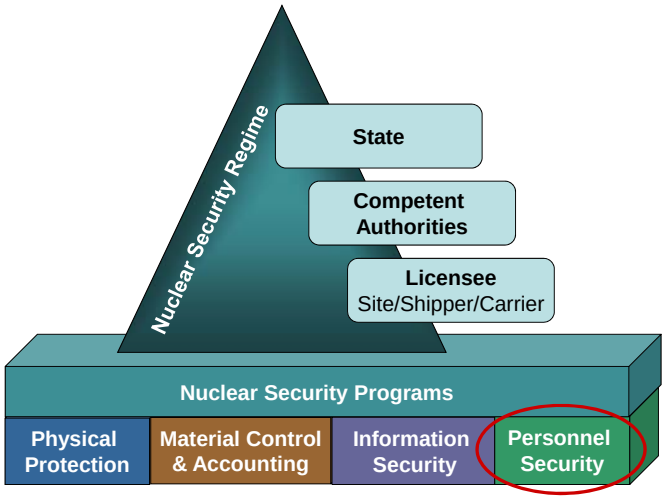
42

Information Security Summary

- The consequences of loss of information systems, whether paper or cyber, can be costly
- Ensure access control, cyber systems, and physical protection systems are integrated under a common security umbrella
- Ensure physical protection information systems are kept isolated from other information systems

43

Nuclear Security Reference Model



44

Discussion

- Who is the greater threat - the insider or the outsider?
- Why?

45

Potential for Malevolent Act

Access
Authority
Knowledge

Insider Opportunity

\+

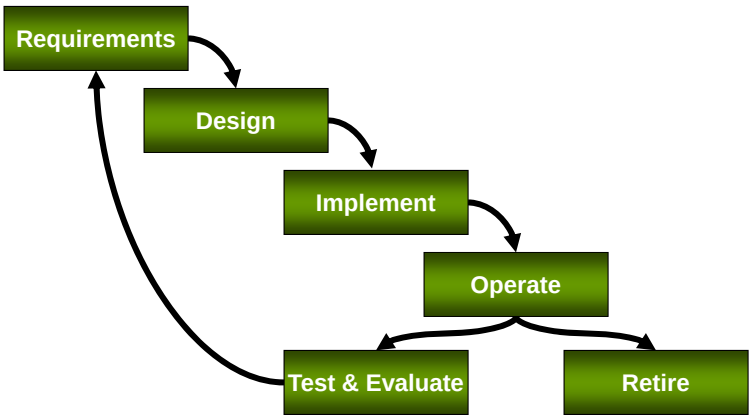
Ideological
Financial
Revenge
Ego
Psychological
Coercion

Insider Motivations

Potential Malevolent Act

46

Facility Life Cycle



Vulnerabilities can be introduced by people at any stage of the system.

47

People – The Human Factor

- Most security assumes that people follow the rules.
- People tend to take the path of least resistance.
- People can be your best detectors or your worst adversaries.
- Contributor to all nuclear security incidents
  - Personnel errors
  - Ergonomic issues
  - Inadequate organizational procedures and processes
  - Management failures

48

Nuclear Security Culture

Ensure all personnel are knowledgeable of and proficient in MC&A requirements:

- Document all requirements in accordance with graded risk dependent upon attractiveness of the nuclear material.
- Proceduralize personnel activities when processing nuclear material to incorporate these requirements.
- Qualification of personnel through a system based on knowledge, experience, and training.

49

Personnel Security Program

- Nuclear Security Culture
  - Shape attitudes and beliefs
- Personnel trustworthiness program
  - Seeks to address motivations
- Graded access control/privileges
  - Least privilege
  - Mitigates access and other insider advantages
- Data monitoring and logging
  - Reduces insider opportunities for malicious activity without exposure

50

Personnel Security Summary

- Elements of a Personnel Security Program
  - Nuclear Security Culture
  - Personnel trustworthiness program
  - Graded access control/privileges
  - Data monitoring and logging
- People are the key to Nuclear Security

51

Decisions to be Made

- Physical protection system
  - Need classification system for protection of information and materials
  - State adopted material categorization definition
  - Define design and evaluation process
- Material control and accounting
  - What material will be accepted in the state
  - Associated material levels of protection
  - Material accounting system
  - Material control system

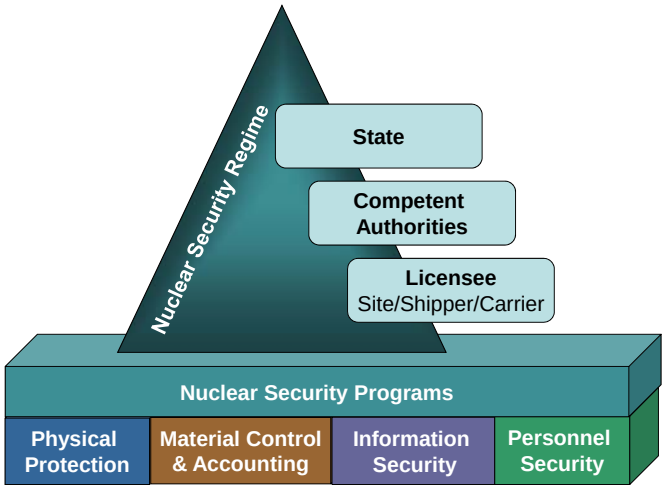
52

Decisions to be Made (continued)

- Information Security
  - Classification system for information and materials
  - Process of certification and accreditation of information system
  - Process for evaluation of information systems
  - Separation of information systems
- Personnel Security
  - Personnel trustworthiness program
  - Personnel identification system
  - Access and privileges levels

53

Summary



54

Conclusion

Questions before we continue?

55

Infrastructure Development: Initiating a Physical Protection Program

Module 6:
Requirements Definition –
Targets and Threats

1

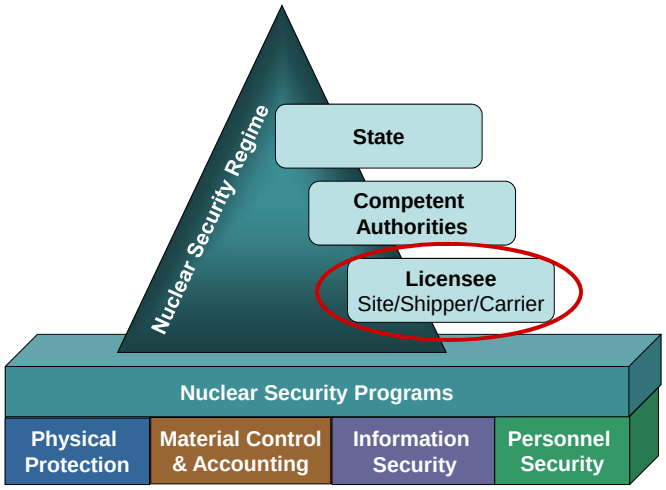
Module Objectives

After completing this module you should be able to do the following:

- Identify the three questions used to define PPS requirements
- Identify the targets of concern in PPS design
- Define design basis threat (DBT)
- Explain how performance requirements are specified

2

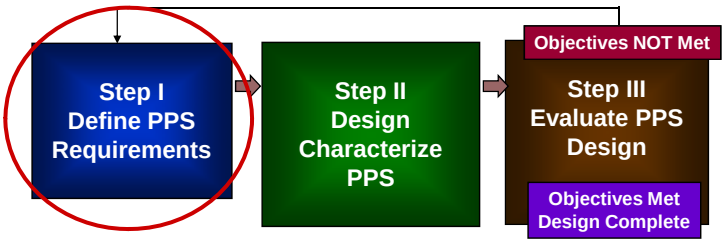
Nuclear Security Regime



3

A System Engineering Process

- Three interdependent steps required



Repeat process until risk is acceptable (iterative process)

4

Three Essential Questions that define the requirements for a PPS

1. What assets must be protected to prevent undesired consequences?
2. What threat must be protected against?
3. What level of protection is adequate?

5

1. What must be protected?

- Nuclear materials
- Nuclear facilities
- Information
- Radioactive sources in the facilities
- People
- Environment

6

Some Undesired Consequences of Malicious Acts

- Damage to national security
- Successful terrorist attack
- Loss of control of nuclear material or weapons
- Loss of life as a result of hazardous material release
- Theft of material or information
- Interruption of critical utilities such as water, power, or communications
- Degraded business operations
- Loss of market position
- Workplace violence, extortion, blackmail
- Damage to reputation
- Legal liability

7

Examples of Metric of Undesired Consequences

- Injury
  - Number of injuries
  - Severity of injuries
- Environment
  - Total hectares contaminated
  - Value of hectares
  - Loss of use
- Political
  - Stability of government
  - Public trust
- Economic - Costs of Act
  - Cleanup and food embargo
  - Loss in productivity
  - Legal costs
  - Value of facilities, etc., damaged
  - Ransom

8

Targets—What are they?

- Theft Targets
  - Nuclear or radioactive materials
  - Information
  - People
- Sabotage Targets
  - Nuclear or radioactive materials
  - Process or support equipment needed to prevent unacceptable radiological consequences

9

IAEA Categorization of Nuclear Material

Material	Form	Category I	Category II	Category III[c]
1. Plutonium[a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235	Unirradiated[b] – uranium enriched to 20% ^{235}U or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15 g
	– uranium enriched to 10% ^{235}U but less than 20% ^{235}U		10 kg or more	Less than 10 kg but more than 1 kg
	– uranium enriched above natural, but less than 10% ^{235}U			10 kg or more
3. Uranium-233	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated Fuel (The categorization of irradiated fuel in the table is based on international *transport* considerations. The State may assign a different category for domestic use, storage, and *transport* taking all relevant factors into account.)			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[cde]	

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/hr
[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.
[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.
[e] Other fuel which by virtue of its original material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/hr (100rad/hr) at one meter unshielded.

10

Categorization Table for Radioactive Materials

Category	Source	A/D	Security level
1	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	A/D ≥ 1000	A
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D ≥ 10	B
3	Fixed industrial gauges that incorporate high activity sources Well logging gauges	10 > A/D ≥ 1	C
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D ≥ 0.01	Apply measures as described in the Basic Safety Standards [5]
5	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt	

11

2. What threats must be protected against?

- The competent authority must define a threat that the physical protection system (PPS) is expected to withstand.
- The defined threat specifies the adversary attributes and characteristics that the PPS must be designed to defend against.
- This is commonly referred to as the design basis threat (DBT).

12

Definitions

Threat Spectrum

A range of adversary types (may be low to high) against which the site and assets will be analyzed (should include maximum credible adversary). May be outsider or insider.

State Threat Assessment

A judgment, based on analysis of available intelligence, law enforcement, and open-source information, of the actual or potential threat to one or more facilities or programs.

Design Basis Threat

A selected threat defined by attributes and characteristics against which a physical protection system is designed and evaluated. Only for high consequence facilities.

13

Definitions

High Consequence Facility

Those facilities whose failure or disruption could be potentially associated with the highest possible impact among all the facilities.

Much of this determination will be a function of the risk tolerance of the enterprise that owns the facilities, but some facilities have an unacceptably high consequence of loss and must be protected.

- Damage to national security
- Successful terrorist attack
- Loss of control of nuclear material or weapons
- Loss of life as a result of hazardous material release
- Loss of market position

14

Design Basis Threat

- State regulatory tool used for planning, designing, and evaluating a PPS (Cat I and nuclear power plant)
- Four components:
  - Malicious acts (theft, sabotage) and unacceptable potential consequences
  - Threat spectrum of potential insider/external adversaries
  - Adversary attributes and characteristics
  - Performance basis for design and evaluation
- Not an explicit description of the expected adversary:
  - Provides basis for State-wide consistency
  - May change as events occur
  - Supports prudent (less than Cat III) PPS within cost constraints

15

The Value of a Design Basis Threat (DBT)

The DBT provides a rational basis for the following:

- Making and justifying decisions
  - By the operators
  - By the competent authority
- The design of a physical protection system
  - Ensuring sufficient countermeasures
  - Avoiding unnecessary countermeasures
- Evaluating the adequacy of a physical protection system

16

Categories of Adversary

- Outsider Threat
  - Protestors, terrorists, criminals
- Insider Threat
  - Act alone or in collusion with external threat
  - May be passive or active
  - May be violent or nonviolent
- Collusion

17

Threat Characteristics – Outsider

- Outsider: Any individual (or group of individuals) without authorized access to nuclear facilities or transport who might attempt unauthorized removal or sabotage, or who might assist insiders in these activities.
- Outsiders might include
  - Terrorists
  - Criminals
  - Protesters
  - Others

18

Example DBT Outsider

- Four well-trained terrorists with military weapons and explosives, plus all commercially available hand and power tools
- Two criminals with handguns and small hand and power tools
- Six protesters with hand and power tools
- Intention: unauthorized removal of radiological materials
- Add tools inside facility
- Collusion: possible with an employee

19

Threat Characteristics – Insider

- **Insider:** Any individual (or group of individuals) with authorized access to nuclear facilities or transport who might attempt unauthorized removal or sabotage, or who could aid outsiders in these activities.
- Insiders might include
  - Management
  - Regular employees
  - Security personnel
  - Service providers
  - Visitors
  - Inspectors
  - Former employees

20

Example DBT Insider

- Number: one in any position
- Type: up to and including active-violent
- Intention:
  - Steal material
  - Commit radiological sabotage against facility and personnel
- Collusion: acts alone while on-site
- Equipment:
  - Tools existing in facility
  - Contraband brought into facility, including small arms or explosives

21

Identify What Needs to be Known About the Threat

- Motivation
  - Ideological, Personal, Economic, Psychotic, or Other
- Intention
  - Theft or Sabotage
- Capabilities
  - Group Size
  - Weapons
  - Explosives
  - Tools
  - Transportation
  - Skills
  - Funding
  - Collusion with Insider
  - Support Structure

22

Maintaining a DBT

- Formal review process should be used to ensure validity of DBT
- Triggers for DBT review include
  - Event that indicates unexpected threat
  - Change in government policy
  - Change in nuclear program
  - Change in nuclear material
  - Request by interested party
  - Periodic review
- Same process is used as for developing a DBT
- Review may or may not result in change to DBT

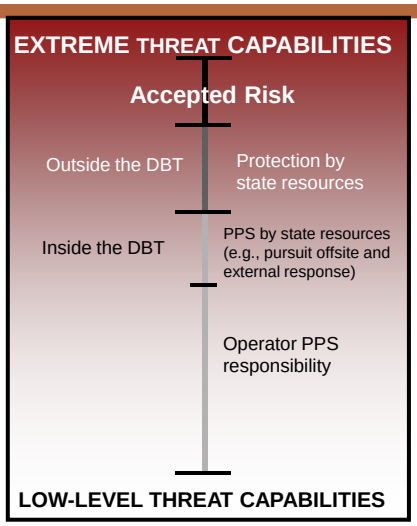
23

3. What level of physical protection is adequate?

- Objective: reduce the risk associated with use of nuclear or other radioactive materials to an acceptable level
- Must strike a balance between risk, beneficial use, and costs
- The level of security should reflect the potential consequences of misuse of the source: higher potential consequences imply higher levels of security (i.e. graded approach)

24

DBT Space



25
25

Decisions to be made

- What needs to be protected?
- What threats to protect against?
- What level of protection is adequate?

26

Summary

- PPS Requirements Definition
  - What must I protect? (targets)
  - What must I protect against? (threat)
  - What level of protection is adequate? (risk/graded approach)
- Targets of concern include nuclear materials and facilities and radioactive materials.
- The DBT is the set of threat characteristics a physical protection system is designed to counter in order to prevent undesired consequences.
- Performance requirements may be feature-based (prescriptive), performance-based, or a combination of both of these approaches.

27

Conclusion

Questions before we continue?

28

Infrastructure Development Initiating a Physical Protection Program

Module 7:
Facility Characterization and Siting Impacts

1

Module Objectives

After completing this module you should be able to do the following:

- Recognize the role of facility siting
- Recognize the role of characterizing a site and physical protection design
- Identify elements of site characterization
- Identify elements of physical protection design characterization

2

Characterization Considerations

- If building a new site, choose the site carefully with physical protection in mind.
- Design the PPS into the site design.
  - This approach is much cheaper than adding the PPS after the site and its facilities have been built.

3

Siting

- Location Considerations
- Environmental Considerations

4

Location Considerations

- Population centers
- Nearby businesses/structures
- Nearest emergency response group
- Security response force location
- Availability and reliability of power and communications
- Proximity to labor pool
- Local crime
- Wide-open spaces

5

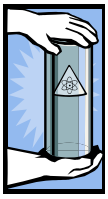
Environmental Considerations

- Topography at the site
- Vegetation and wildlife
- Background noise
- Climate and weather
- Soil conditions
- Water flows/drainage

6

Other Considerations

Safety



Legal

Political

7

The Role of Characterization

- Establishes a baseline
- Provides input to system effectiveness evaluations
- Identifies potential weaknesses in physical protection systems
- Facilities can be characterized using
  - Concept of operations
  - Existing site information
  - Open sources

8

Site Characterization

- Vital Areas
- Physical Conditions
- Operational Conditions
- Non-Standard/Emergency Conditions
- Physical Protection System
- Infrastructure
- Siting

9

Vital Area Identification in High Consequence Facilities

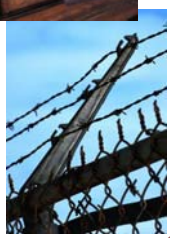
Areas containing

- Nuclear material or other radioactive materials
- Equipment, systems, or devices to be protected against sabotage resulting in
  - Exposure of people to radioactivity
  - Release of radioactivity to the environment

10

Physical Conditions

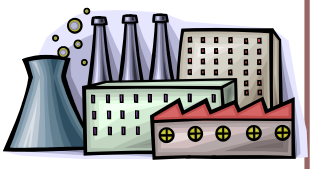
- Site boundaries, fences, barriers,
- Building's construction materials for walls, ceilings, floors, doors, windows, etc.
- Areas and rooms
- Access points
- Environmentally-controlled areas
- Locations of non-target, hazardous material



11

Operational Conditions

- Operational activities
  - Products and processes
  - Operational hours/shifts
  - Number, types, and locations of employees
  - Visitors and vendors
  - Circulation control (access management)
- On-site location and movement of materials



12

Non-Standard/Emergency Conditions

- Equipment failures
- Maintenance
- Medical emergency
- Unusual weather – fog, rain, wind, snow, hurricane, etc.
- Labor dispute
- Fire

13

Physical Protection System

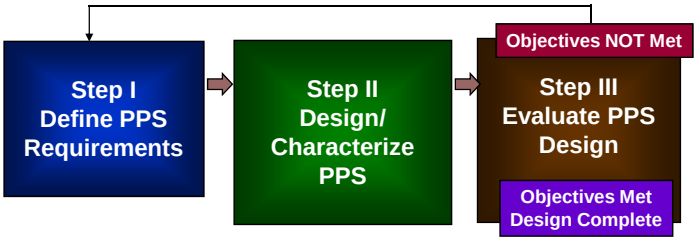
Characterize existing system or new design

- Protection Layers
- PPS Functions
  - Detection and Assessment
  - Delay Mechanisms
  - Response
- Policies and Procedures

14

A System Engineering Process

- Three interdependent steps required:

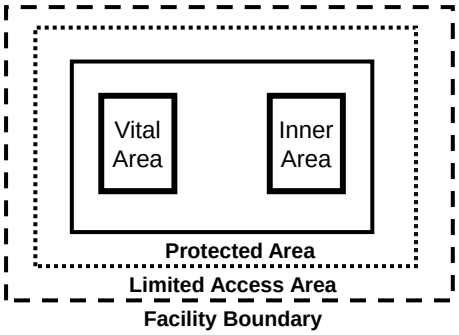


Repeat process until risk is acceptable (iterative process)

15

Identify Protection Layers and Associated Security Areas

- Typical Layers:
  - Limited access area
  - Protected area
  - Inner area
  - Vital area



- Some protection systems may have more or fewer areas.

16

Facility Policies and Procedures

- Written and unwritten policies/procedures
  - Frequently, procedures in use are not implemented as described in the documentation.
- Training security policies and procedures
- Other indications of nuclear security culture

17

Infrastructure

- Availability and reliability of the following:
  - Heating, ventilation, air conditioning
  - Communication paths and types
  - Power distribution system

18

Decisions to Be Made

- Facility Siting
- Security areas and layers of protection
- Targets and target locations
- Detection and assessment
- Access control system
- Delay mechanisms
- Response force capabilities

Module Summary

- Characterization involves gathering data that impacts the performance of the PPS such as:
  - Vital Areas
  - Physical Conditions
  - Operational Conditions
  - Non-Standard/Emergency Conditions
  - Physical Protection System
  - Infrastructure
  - Siting
- Siting greatly affects physical protection systems.

20

Conclusion

Questions before we continue?

21

Infrastructure Development: Initiating a Physical Protection Program

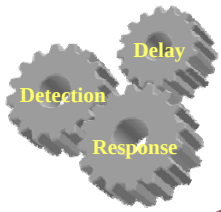
Module 8:
Detection, Delay, and Response Overview

1

Module Objectives

After completing this module you should be able to do the following:

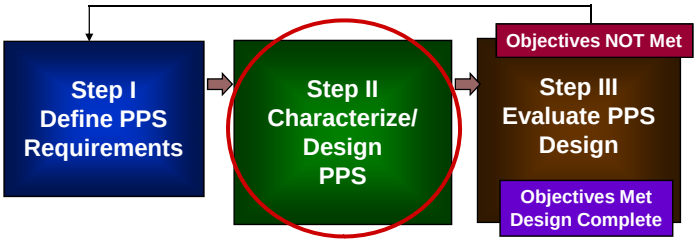
- Explain the three integrated components of Physical Protection System (PPS)
- Discuss the relationships between them
- Explain the characteristics of an effective PPS



2

A System Engineering Process

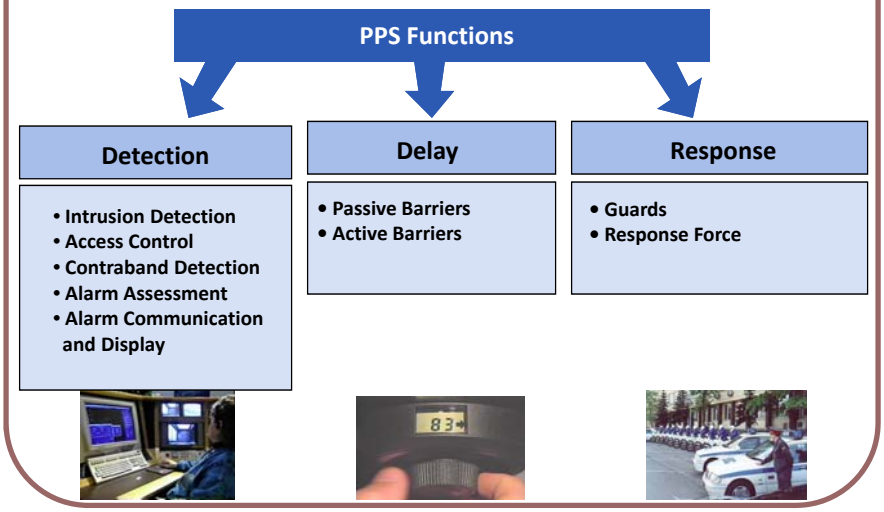
- Three interdependent steps required:



Repeat process until risk is acceptable (iterative process)

3

PPS Functions



4

Security Event Sequence Example

- Adversary begins attack.
- Perimeter sensor detects an intrusion.
- Security operator assesses the alarm as an intrusion and initiates response.
- Response forces gear up and move to respond.
- Meanwhile, adversary is making his way through the facility to his ultimate target.
- He encounters more fences, distance, and barriers before getting to the building that has his target.
- The adversary has a fake credential that he uses to attempt to tailgate an authorized employee through an access control point. The attempt fails, so he must attempt another means to enter or wait for another employee to try again.
- Meanwhile, the security operator is tracking the progress of the adversary and communicating with response forces to direct them to the building.
- Response forces intercept and apprehend the adversary outside of the building.

5

Detection

Sensor Activated → **Alarm Signal Initiated** → **Alarm Reported** → **Alarm Assessed**

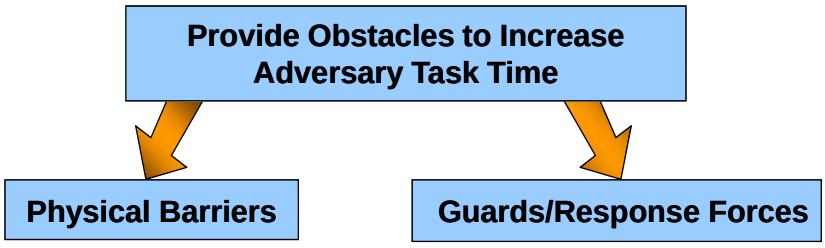
- Performance measures:
  - Time for communication and assessment
  - Frequency of nuisance alarms

- A long time delay between sensor alarm and assessment lowers probability of detection
- People can provide both an alarm and assessment simultaneously

"An alarm without assessment is not detection."

6

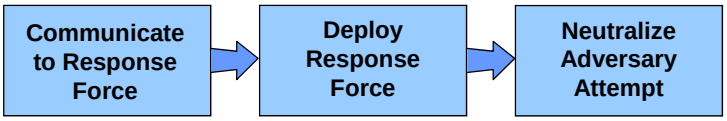
Delay



- Performance measure
  - Time to defeat obstacles
- Delay (to be effective) must occur after detection

7

Response



- Performance measures
  - Probability of communication to response force
  - Time to communicate
  - Probability of deployment to interruption location
  - Time to deploy
  - Response force effectiveness (neutralization)
- Part of the response may be the people who have detected the event

8

PPS Performance Measures

- Detection
  - Timely detection
- Delay
  - Time added to Adversary Task time
- Response
  - Time
  - Effectiveness

9

Relationship of PPS Functions

- System detection and response time must be less than adversary task completion time
- To increase the probability of system success
  - Detect intrusion earlier
  - Reduce assessment time
  - Increase adversary task completion time (add delay)
  - Reduce response time

10

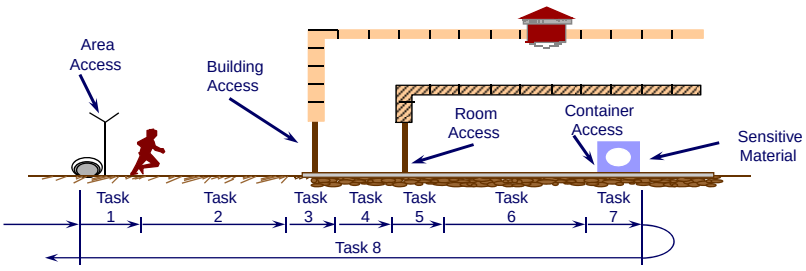
Characteristics of an Effective Physical Protection System (PPS)

- Timely detection and response
- Balanced protection
- Protection-in-depth
- Minimum consequence of component failure
  - Single-point of failure
- Secure by design

11

Timely Detection and Response

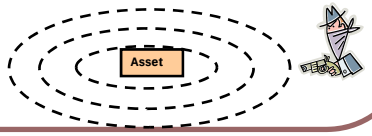
For a successful system design, the total time for detection, delay, and response must be less than adversary task time to complete his or her goal



12

Protection-in-Depth

- Adversary must defeat or avoid a number of protection features in sequence
- Protection-in-depth should
  - Increase adversary's uncertainty about the system
  - Require more extensive preparations by adversary prior to attacking the system
  - Create additional steps where the adversary may fail or abort his mission
  - Require more time for adversary to access target



13

Balanced Protection

- No matter how an adversary attempts to accomplish the goals, effective elements of the PPS will be encountered
- Provides adequate protection against all adversaries along all possible paths
- Maintains a balance with other considerations:
  - Cost, safety, structural integrity, operations, etc.

14

Minimum Consequence of Component Failure

- Compensatory measures must be provided so that the PPS continues to operate after a component fails
- Redundant equipment can take over the function of disabled equipment in some cases
  - e.g., backup power exists if primary power is lost
- Some failures require aid from sources external to the facility
  - e.g., National Guard is used to supplement security during times of higher alert status (i.e., replace sensors with manpower)

No single-point failures

15

Secure by Design

Security is

- Integrated into the site design process
- Essential to the mission of the facility
- Built into the system during construction
- A part of the culture

16

PPS Overview Summary

- PPS consist of
  - Detection
  - Delay
  - Response
- Characteristics of an effective PPS
  - Secure by design
  - Protection-in-depth
  - Minimum consequence of component failure
  - Balanced protection
  - Timely detection and response
- The total time for PPS detection, delay, and response must be less than adversary task time to complete his or her goal

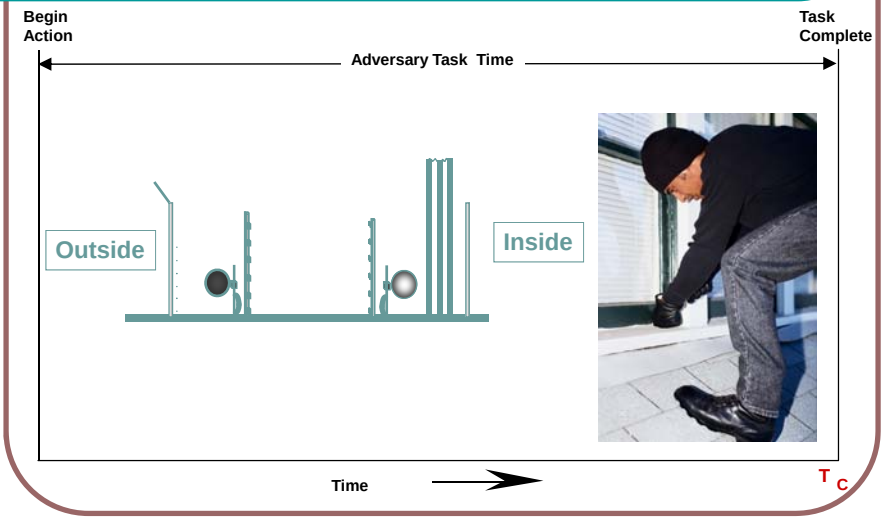
17

Conclusion

Questions before we continue?

18

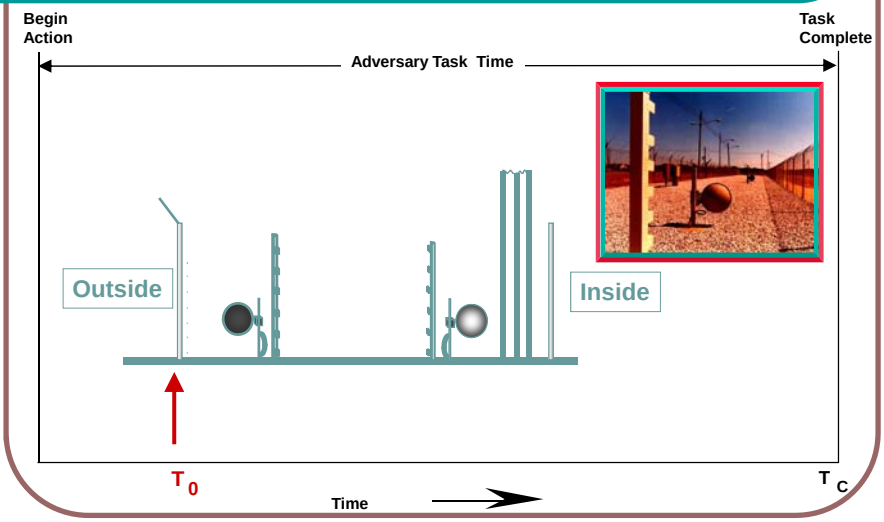
Traditional Adversary Task Time



T_C = Adversary task completion time

19

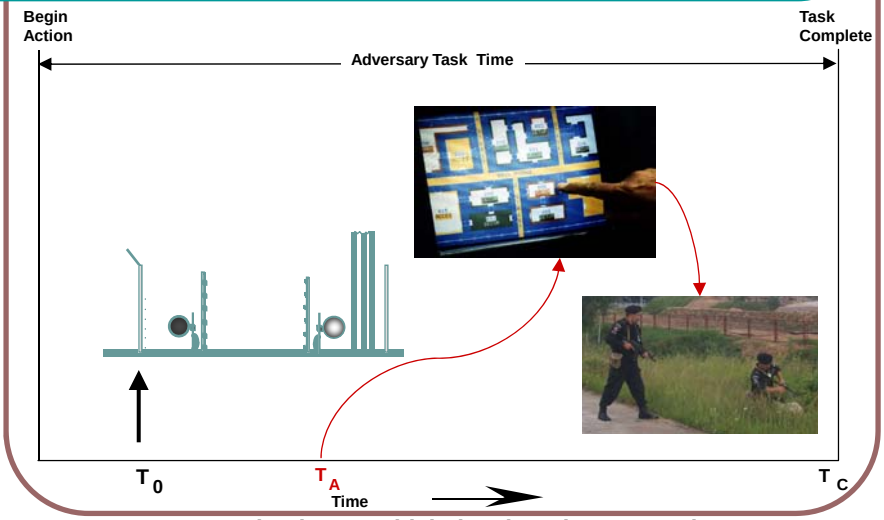
Security Event Start



T_0 = First alarm occurs and is communicated to Central Alarm Station

20

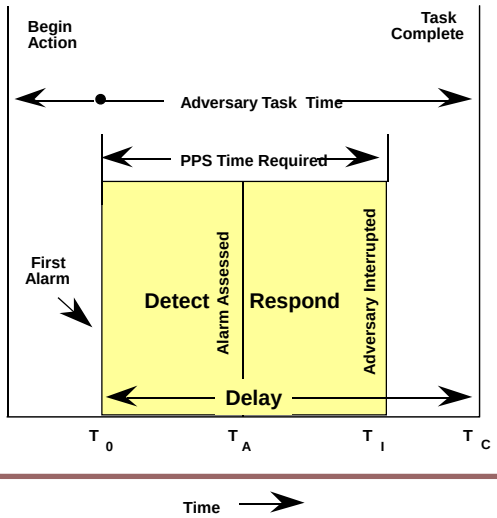
Alarm Assessed and Response Initiated



T_A = The time at which the alarm is assessed to be valid and response initiated

21

Traditional Adversary Task Time vs. PPS Time Requirements



T_0 = First alarm occurs

T_A = The time at which the alarm is assessed to be valid

T_I = The time at which the response force interrupts adversary actions

T_C = Adversary task completion time

22

Physical Protection Systems Elements

Module 9:
Intrusion Detection

1

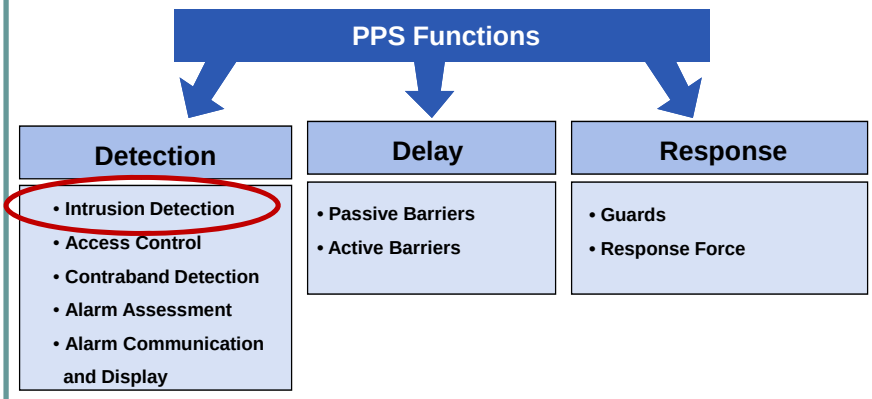
Module Objectives

After completing this module, you should be able to do the following:

- Identify the role of Intrusion Detection in a PPS
- Discuss types of Intrusion Detection sensors
- Identify the performance characteristics of Intrusion Detection sensors
- Discuss characteristics of a good design

2

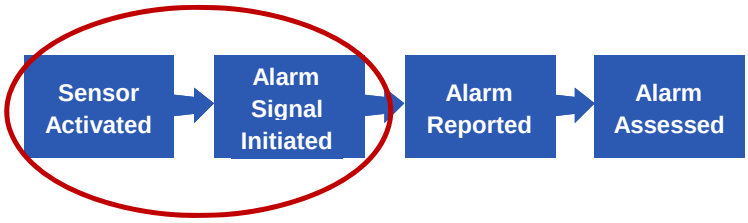
Role of Intrusion Detection



- **Detection – a process that begins with sensing a potentially malicious or unauthorized act and completed with the assessment of the cause of the alarm**

3

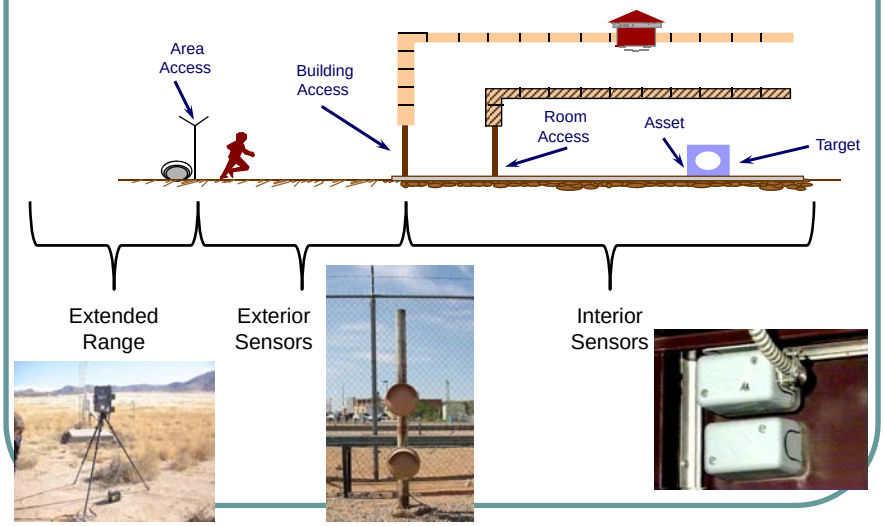
Detection Process



- Intrusion Detection includes the activation of the sensor and the initiation of the alarm signal

4

Types of Sensors



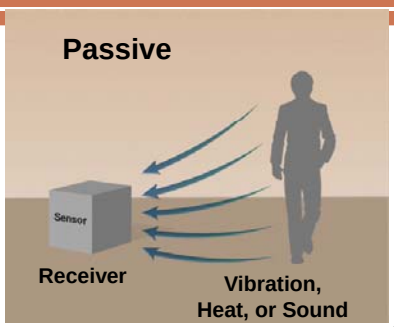
5

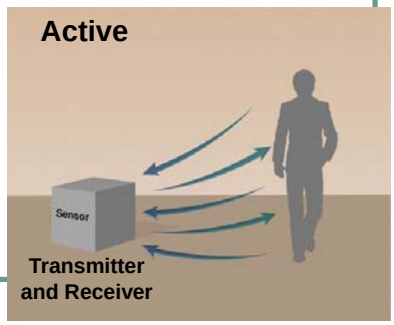
Sensors Features

- Passive or Active
- Covert or Visible
- Volumetric or Line Detection
- Line-of-Sight or Terrain-Following

6

Passive or Active

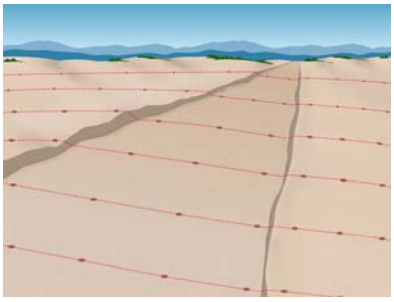




7

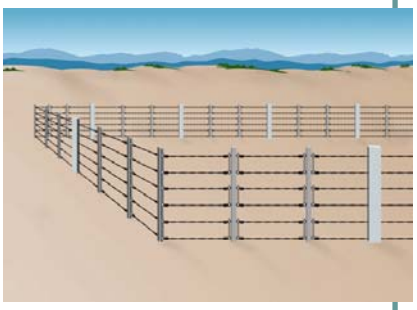
Covert or Visible

Covert



- Sensors hidden from view
- More difficult for intruder to detect

Visible

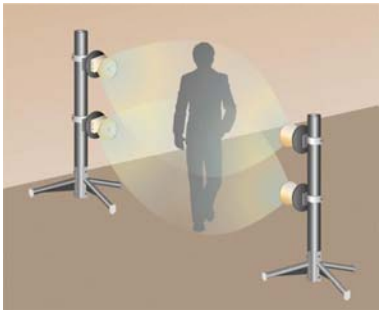


- Sensors in plain view of intruder
- Simpler to install and repair

8

Volumetric or Line Detection

Volumetric



- Detection in a volume of space
- Detection volume is not visible

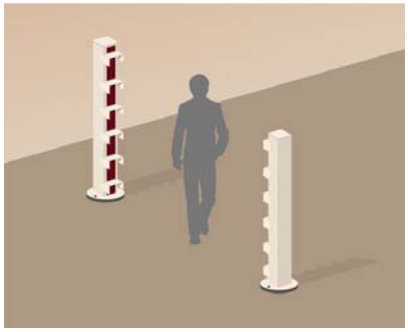
Line Detection

- Detection along a line or plane
- Detection zone easily identified

9

Line-of-Sight or Terrain-Following

Line of Sight



- No obstacles in the detection space
- Requires flat ground surface

Terrain Following

- Sensors detect over flat or irregular terrain

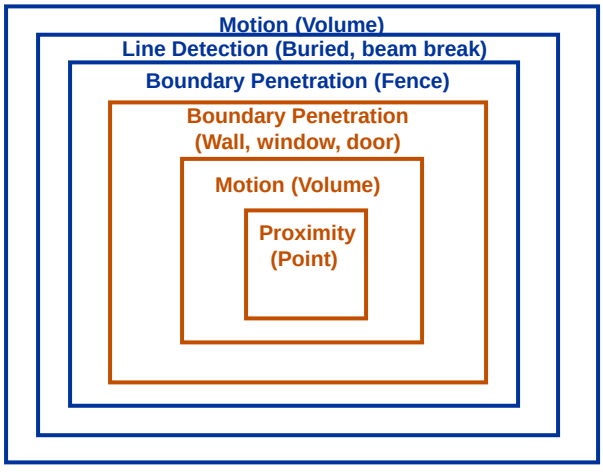
10

Characteristics of Intrusion Detection

- Performance characteristics of Intrusion Detection
  - High probability of detection
  - Not vulnerable to defeat
  - Low Nuisance and False (i.e., unknown) Alarms
- High Probability of Detection - sensor location and selection that are highly likely to detect an intruder
  - Detection in Depth – multiple and complementary sensors
  - Site-specific System – sensor selection
  - Dependent on Adversary Capabilities
  - Use Performance Testing to Determine

11

Protection-in-Depth

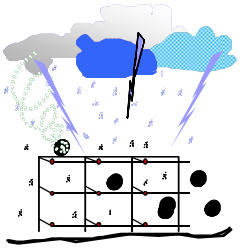


12

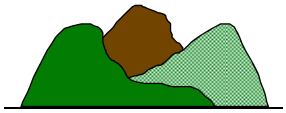
Environmental Dependencies

- Physical environmental conditions
- Industrial environment

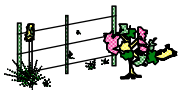
Climate and Weather

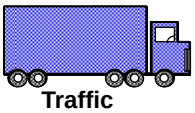


Topography

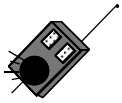


Vegetation





Traffic



Noise – sound or electromagnetic

Wildlife

13

Site-Specific Dependencies

- Site protection requirements – DBT
- Integration with Assessment System
  - Video capabilities
  - Response force

Response Force

Video

14

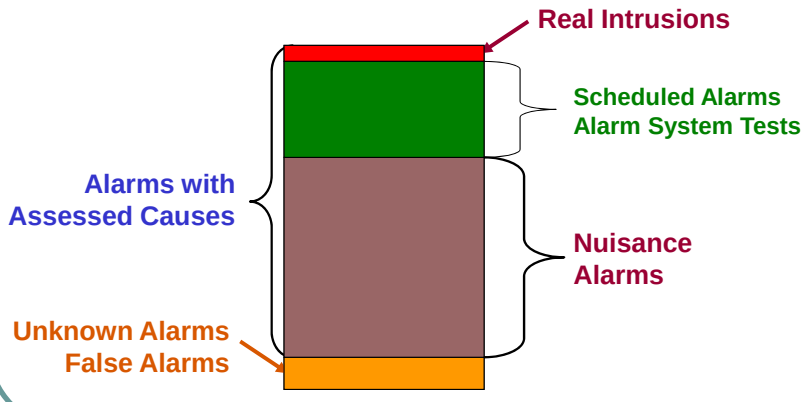
Vulnerability to Defeat

- Adversary Tactics
  - Bypass: avoiding the detection volume of the sensor by crawling, jumping, tunneling, or bridging
  - Spoofing: tricking the sensor into not reporting an alarm
- Given proper knowledge, tools, and time, every sensor can be individually defeated

15

Performance Characteristics

Causes of Alarms



16

Characteristics of a Good Design

- Design to highest probability of detection with a minimum of nuisance alarms
- Design to minimize vulnerability to defeat
  - Integration with the barrier system
  - Continuous line of detection with overlapping detection zones
  - Protection of system and system components
  - Use of complementary and different types of sensors
  - Sensor selection for physical and industrial environment
- Integrated with Alarm Assessment System

17

Decisions to Be Made

- Siting of facility to facilitate detection systems
- Covert versus visible detection
- Performance test requirements
- Detection system requirements – exterior/interior
- Sustainability

Summary

- Intrusion Detection is one element of the PPS function of Detection and includes activation of the sensor and the initiation of the alarm signal.
- Types of sensors: exterior, interior, extended range.
- Performance characteristics include Probability of Detection, Vulnerability to Defeat, and the Nuisance Alarm Rate.
- A good sensor design has a high probability of detecting intruders with minimum of Nuisance Alarms

19

Conclusion

Questions before we continue?

20

Physical Protection Systems Elements

Module 11:
Access Control Systems

1

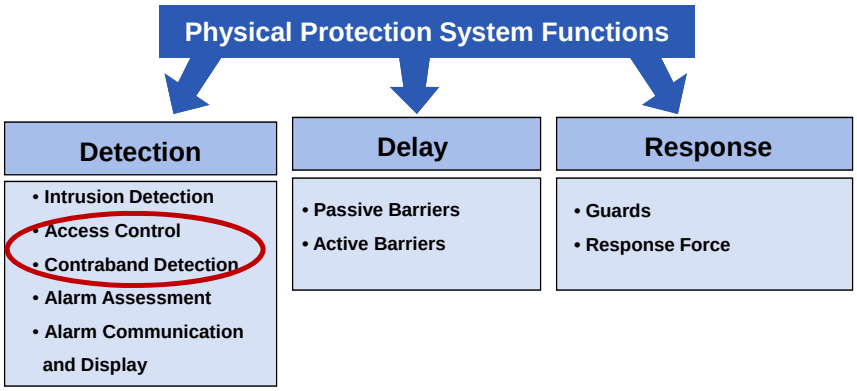
Module Objectives

At the completion of this module, the student will be able to do the following:

- Define Access Control, Entry Control, and Contraband Detection
- Identify 3 Levels and 3 Types of Access Verification
- Identify types of Contraband Detection
- Discuss Features of a Good Access Control System
- Describe Performance Measures

2

Role of Access Control



- Access Control and Contraband Detection are elements of the PPS function of Detection.

3

Role of Access Control

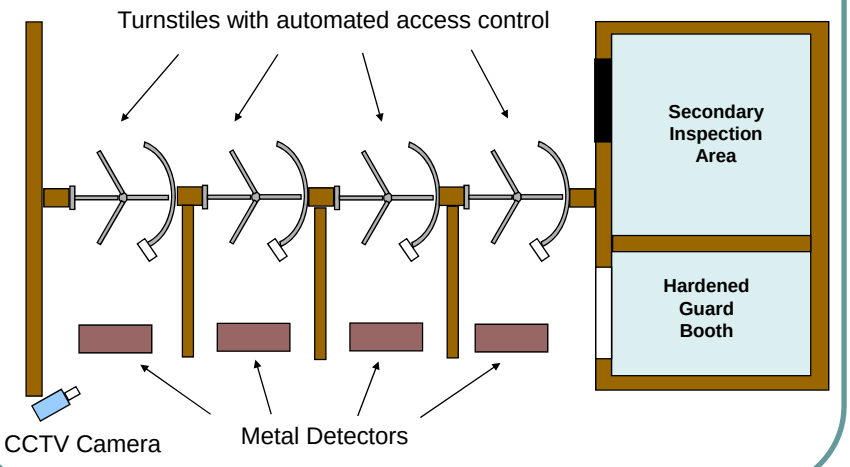
- A perimeter security system provides a boundary around each protection layer to prevent or detect unauthorized penetrations.
- Access Control allows authorized persons, packages and vehicles to move in and out through that boundary.
- Access Control must also prevent entry of unauthorized persons, packages, and vehicles

4

Role of Access Control

5

Access Control Systems – An Example



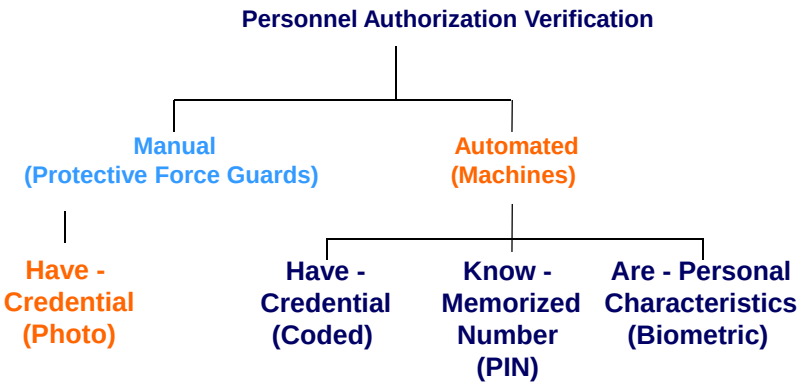
6

Definitions for Access Control

- **Access Authorization** – an administrative determination that an individual is eligible for access to nuclear material or classified matter
- **Badge** - credential an individual is provided once access authorization is determined
- **Verification** – determination of access authorization and identity at the access control point
  - Accepts authorized persons or vehicles
  - Rejects unauthorized persons or vehicles

7

Access Control Personnel Verification Types

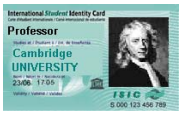


8

Types of Automated Access Control

Automated (Machines)

Have - Credential (Coded)	Know - Memorized Number (PIN)	Are – Personal Characteristics (Biometric)
• Photo badge • Exchange badge • Coded credential • Key	• Uniqueness of the PIN • Number of digits • System used to enter PIN	• Fingerprint • Hand geometry • Retinal pattern



Levels of Access Control

Level	Verification	Examples
1	One type	Credential **OR** PIN
2	Two Types	Credential **AND** PIN OR Credential **AND** Biometric
3	Three Types	Credential **AND** PIN **AND** Biometric

10

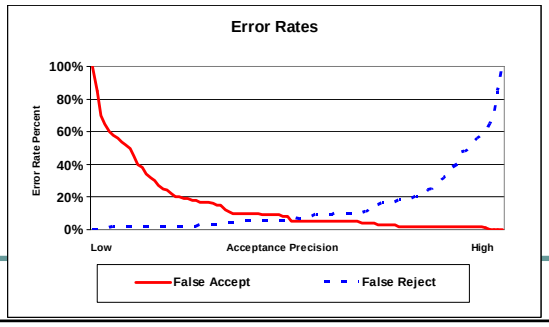
Features of a Good Access Control System

- Implements site requirements for limiting access per access authorization
- Integrated with Physical Boundary
  - Personnel and Vehicle Entry
    - Blocks passage until access verification is complete
    - Provides secondary inspection and verification for specialty cases
    - Procedures for non-standard and emergency conditions
  - Interfaces with Intrusion Detection System

11

Performance Measures of Access Control

- Performance measures of Access Control are
  - Throughput – measure of the time for an authorized person to successfully pass an entry or exit point
  - Error Rates
    - Type 1 – False Reject (someone with authorization cannot get in)
    - Type 2 – False Accept (someone without authorization gets in)



12

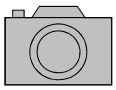
Dual Role of Contraband Detection

Allow entry of • **Authorized material**	**Prevent entry of** • **Weapons** • **Explosives** • **Other contraband**
Allow exit of • **Authorized material**	**Prevent unauthorized exit (theft) of** • **Nuclear Material**

13

What is Contraband?

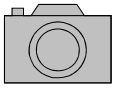
- Contraband is any object deemed “prohibited” for a site, facility, or area
- Contraband is any item that would permit theft of any controlled item

14

Contraband Distinctions

- Prohibited vs. Controlled items
  - Prohibited – not allowed
  - Controlled – allowed by certain people or under certain circumstances
    - Examples
      - Response force weapons
      - Radioactive sources for calibration of equipment
  - Personally-owned vs. site-owned (business-use) items



15

Contraband Detection Inspection

People

Walk-through Systems

Things

Package Inspection

Vehicles

Portals or Stationary Inspection

Decisions to Be Made

- Minimum number of access points for each protection layer
- Type of access control to be employed – technology, manpower, combination
- Adequate infrastructure to support access control
- Emergency situation management
- The need for contraband detection (entry/exit)
- Contraband materials list

Summary

- Access control limits the entry into and exit out of a site, facility, or area
- Entry control limits the flow of people
- Contraband detection detects entry and exit of unauthorized material
- Features of a good Access Control system include
  - Implements site requirements for limiting access per access authorization
  - Integrated with Physical Boundary
  - Procedures for non-standard and emergency conditions
- The Performance Measures for Access Control are throughput and error rates

18

Summary

- There are three types of access control verification:
  - What you have – credential
  - What you know – PIN
  - What you are – biometric
- There are three levels of access control
  - Level 1 – credential **OR** PIN
  - Level 2 – credential **AND** PIN OR credential **AND** biometric
  - Level 3 – credential **AND** PIN **AND** biometric
- There are three types of contraband detection
  - Persons
  - Packages
  - Vehicles

19

Conclusion

Questions before we continue?

20

Physical Protection Systems Elements

Module 11:

Alarm Assessment, Communication and Display

1

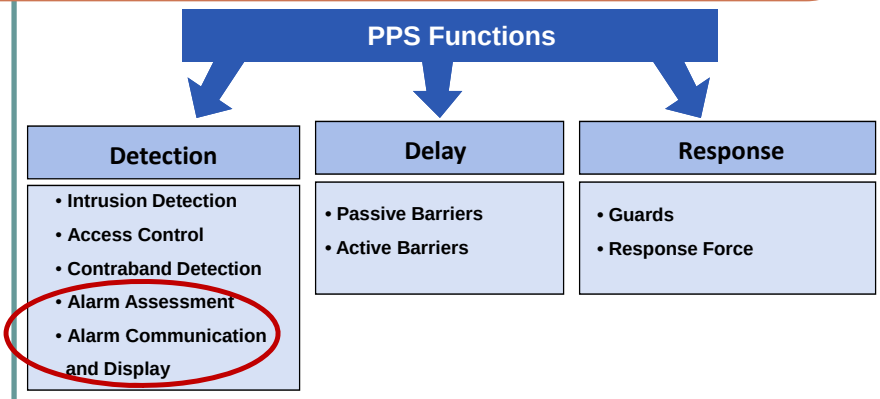
Module Objectives

After completing this module, you will be able to do the following:

- Describe the purpose of alarm assessment
- Identify two methods of alarm assessment
- Describe differences between assessment and surveillance

2

Role of Intrusion Detection



- Alarm Assessment and Alarm Communication and Display are elements of the PPS function of Detection.

3

Role of Assessment

- Detection Process

  - Detection is the notification that a possible security event is occurring.
  - Assessment is the act of determining whether the event is an attack or a nuisance alarm.

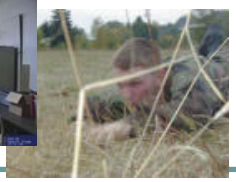
- Detection is not complete without assessment.

4

Purpose of Alarm Assessment

- Determine the cause of each sensor alarm
  - Intrusion Alarm – threat
  - Nuisance Alarm – other assessed causes
  - False Alarm – undetermined causes
  - Scheduled Alarm – maintenance or test
- Provide details for response
  - Who
  - What
  - Where
  - How Many



5

Methods of Alarm Assessment

Guard/Response Force

Elevated towers or dispatched patrols


Disadvantage: Delay between alarm and eyes on area for assessment

Video System Display

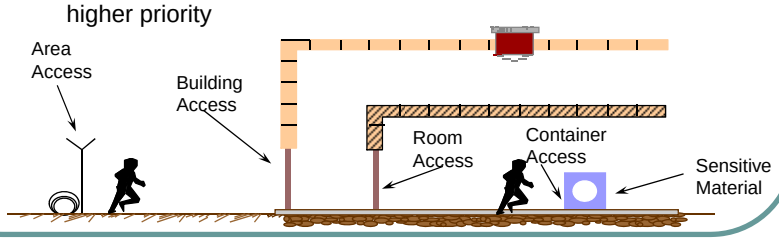
Central Alarm Station: Stationary Cameras or Extended Range Imager


Disadvantages: cost of infrastructure and maintenance; Response Force assessment may still be required

6

Methods for Alarm Assessment

- Alarm Prioritization
  - Alarms and associated video displayed at alarm monitoring station commonly displayed by priority and time
  - Types
    - Simple static – sensors closest to asset given higher priority
    - Dynamic or groups of sensors – multiple alarms in one area given higher priority



7

Is there a potential threat in perimeter?

8

Is there a potential threat in perimeter?

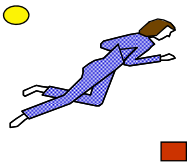
9

Is there a potential threat in perimeter?

10

Resolution

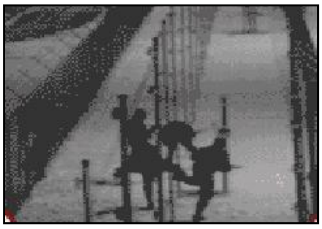
- Resolution is the degree to which you can see fine details in viewed image
- What you see depends on camera resolution, size of the object, contrast, and motion of the object.

Detection	Classification	Identification
		
Determine Presence of Object	Determine Nuisance or Real Alarms	Determine Identity of Object

11

Video Assessment

- **Video Assessment** – alarm-initiated video of a sensor detection zone at the time of an intrusion alarm



- Video assessment is integral to the Alarm Communication and Display (AC&D) system

12

Surveillance

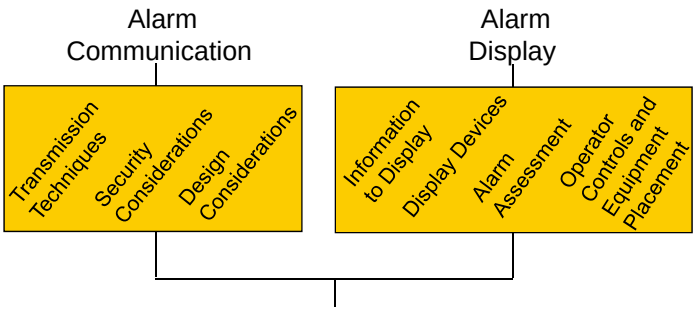
- **Surveillance** – continuous video monitoring of activity in an area without benefit of an intrusion sensor to direct attention to a specific event or area

- Surveillance is also integral to the Alarm Communication and Display (AC&D) system

13

Objectives of AC&D

Two components of AC&D Systems



14

Types of Alarm Monitoring Stations

- Simple system
  - Annunciator Panel with status lights or simple computer text/graphic display

15

Types of Alarm Monitoring Stations

- Complex system
  - Integrated systems – entry control, alarm system, and video system, networked to PC-based display system

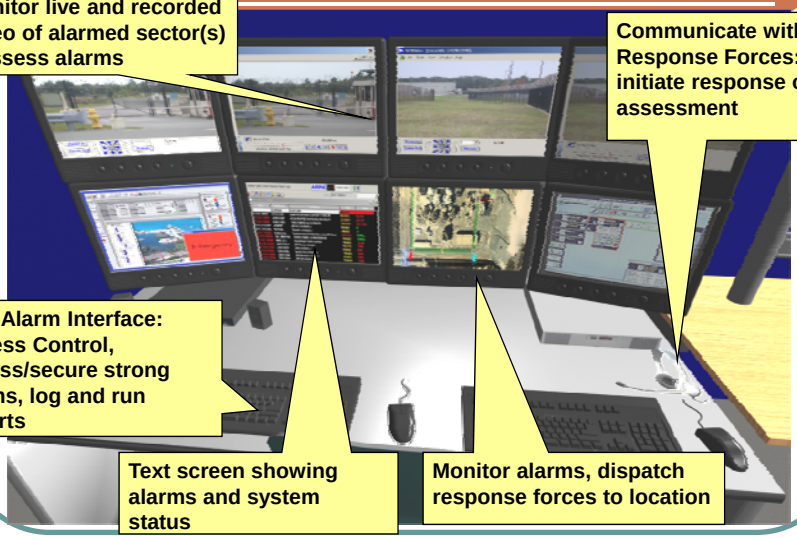
16

Features of Alarm Monitoring Station (AMS)

- Provides overall status of site “Security System”
  - Alarm annunciation – audible and visual, location
  - Video displays
- Provides effective communication between AMS and Protective Forces
- Interfaces with Access Control
- Robust and reliable system
- Has protection measures for system components and information
- Designed for ergonomics
  - Number of alarm monitoring station operators
  - Information management
    - Presents information quickly and effectively
    - Logs information

17

Operator functions of AC&D



18

Decisions To Be Made

- Assessment using technology or manpower
- Complexity of the alarm monitoring station
- Alarm prioritization
- Alarm control and display system specifications
- Resolution of video

Summary

- Alarm assessment is to determine whether an alarm is a threat or nuisance alarm.
  - Detection is not complete without assessment.
- Alarm Assessment is either by Response Forces or Video Assessment.
- Video Assessment and Video Surveillance:
  - Assessment is alarm-initiated video display of a sensor detection zone.
  - Surveillance is continuous video display, which may or may not be observed at any given time.

20

Conclusion

Questions before we continue?

21

This page intentionally left blank.

Physical Protection Systems Elements

Module 12:
Access Delay Systems

1

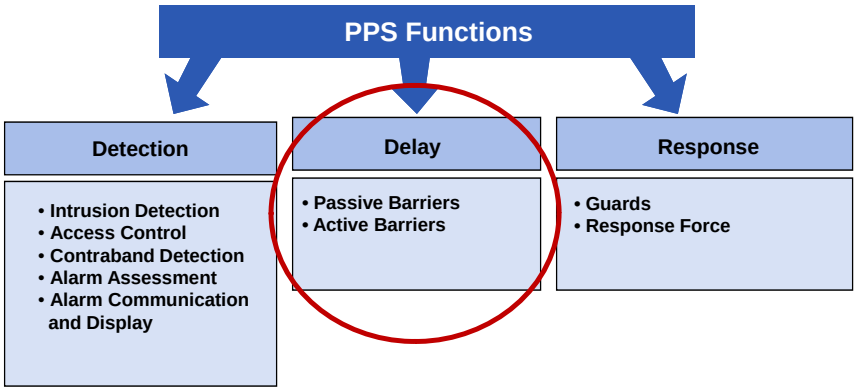
Module Objectives

After completing this module you should be able to do the following:

- Describe the purpose of Access Delay Systems
- Explain why detection must occur before delay
- List three characteristics of a good barrier design
- Recognize the definition of penetration

2

Role of Detection

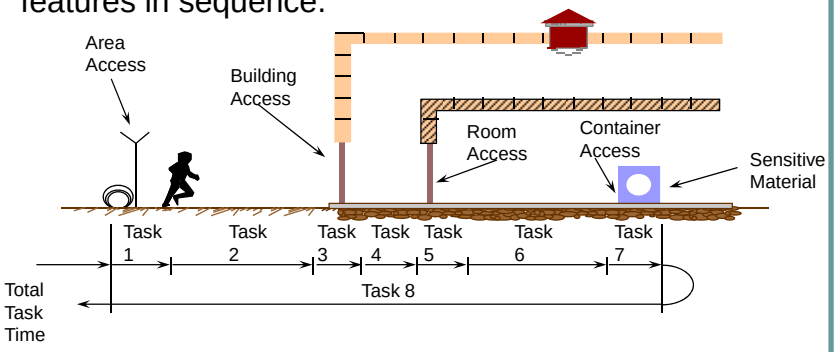


- Access Delay Systems covers the element of the PPS function of Delay.

3

Purpose of Access Delay System

- Adversary must defeat or avoid a number of protection features in sequence.

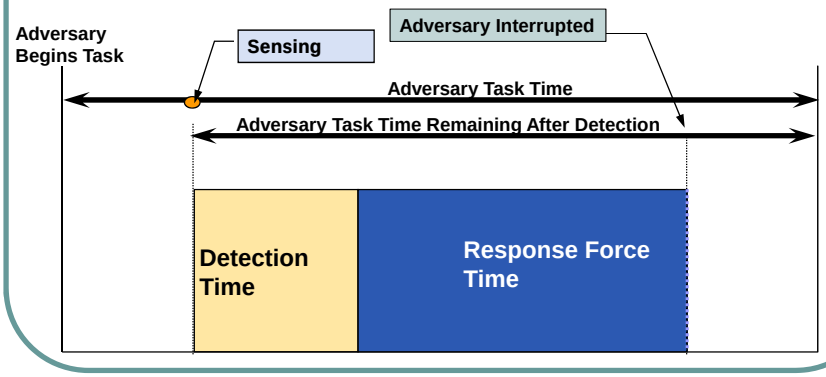


- To be effective, delay must occur after detection.

4

Purpose of Access Delay System

- After detection, delay elements prevent completion of a malevolent act by providing delay until response forces can arrive.



5

Purpose of Access Delay

- Barriers must be considered in relation to the adversary's objective as defined in the DBT.
- Barriers must be in place 100% of the time, or compensatory measures must be taken.

6

Compensatory Measures

- Barriers must be considered in relation to the adversary's objective as defined in the DBT.
- Barriers must be in place 100% of the time, or compensatory measures must be taken.
- Compensatory measures include the following:
  - Personnel entry points: doors or turnstiles
  - Vehicle entry control point: Sally Port configuration; i.e., two barriers in series
  - Vault door: provides added protection; must be guarded when open or accessed

7

Characteristics of Good Access Delay

- Provides Delay after Detection
- Exhibits a balanced design
  - No weak links
  - Considers all adversary paths, tools, and skills
- Employs defense-in-depth by delay-in-depth
  - Different defeat tools and skills
  - Multiple barriers
  - Different barriers

8

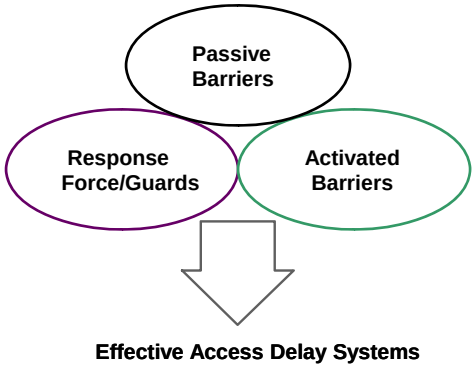
Definition of Penetration

- Penetration is when an individual can pass through, over, under, or around a barrier.
- Penetration times depend on the following:
  - Type of barrier
  - Location of the attack – open area or confined space
  - Tools – hand, power

Possible Adversary Tools

9

Types and Principles for Access Delay



10

Types and Principles for Access Delay

- Passive Barriers include structural elements:
  - Doors, walls, floors, locks, vents, ducts, and fences
  - Always fail secure
  - Conventional construction
    - Provides minimal delay against formidable threat; e.g., explosives
    - Can detain an adversary at predictable locations
  - Upgraded construction
    - Adds some delay
    - Design should maintain balanced protection

11

Types and Principles for Access Delay

- Guards/Response Force
  - Flexible and continuous delay element
  - Provide minimal delay when adversaries use force except when in fixed and protected positions
  - Additional guards used in contingency plans

12

Types and Principles for Access Delay

- Activated Barriers
  - Are not in place until activated by
    - guard
    - intrusion detection
    - combination
  - Include chemical fogs and smokes, foams, and irritants
  - Good for most types of threats
  - Safety considerations for unintended activation

13

Decisions To Be Made

- On-site or off-site response determines the delay necessary
- Passive or activated barriers

Summary

- Access Delay System provides sufficient delay so the response force can arrive before the adversary completes a malevolent act.
- Features of good Access Delay:
  - provides delay after detection
  - exhibits balanced design without weak links
  - employs Delay-in-Depth
  - integrates into access control and detection systems
- Barrier penetration is when an individual can pass through, over, under, or around a barrier.
- Penetration time for the adversary will depend on the type and location of the barrier to be breached and the tools used for breaching.
- Delay elements include passive barriers, guards, and activated barriers.

15

Conclusion

Questions before we continue?

16

Physical Protection Systems Elements

Module 13:
Response

1

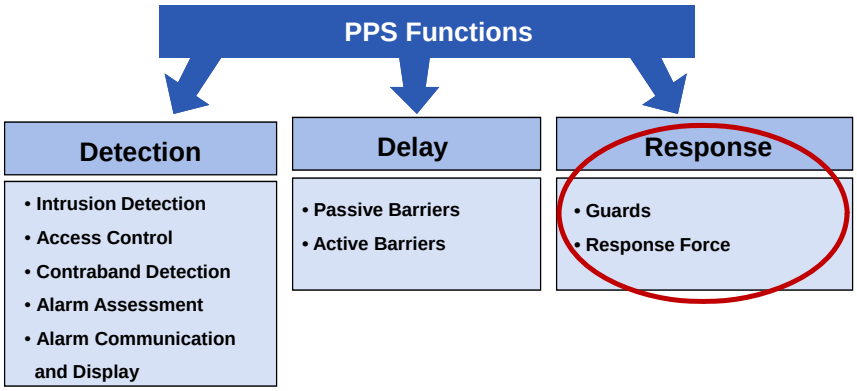
Module Objectives

After completing this module, you should be able to do the following:

- Describe the Role of Response
- Distinguish between guards and response forces
- Discuss levels and strategies
- Describe the roles of command, control, and communication in successful response
- Discuss General Considerations for Response

2

Role of Response



- Response follows Detection and occurs in parallel with Delay.

3

Guards and Response Forces

Guard Forces:
People that perform routine, day-to-day duties

Response Forces:
Persons responsible for the delay, interruption, and/or neutralization of an adversary

- Considerations
  - Staffing the guard and response forces – direct or contract employees
  - Role of support agencies – written agreements
  - Legal Do's and Don'ts
  - Contingency planning
  - Staffing and attrition

4

Role for Response

- **Interruption** – Successful arrival of the Response Force at an appropriate location to capture or detain the adversary
  - Requires
    - Accurate communication to response force
    - Effective deployment of response force
- **Neutralization** – Successfully stops the adversary before the adversary's goal is accomplished
  - Response Force kills, captures, or causes the adversary to flee
  - Use-of-Force continuum

5

Role for Response

- Use-of-Force Continuum

Presence => verbal => use of hands => less lethal => deadly force

=> => => =>

6

Levels for Response

- Use-of-Force Continuum – Presence

7

Levels for Response

- Intermediate force
  - Hand-to-hand combat – control techniques
  - Less than lethal tools
    - Chemicals
    - Tasers
    - Impact Weapons

8

Objectives for Response

- Use-of-Force Continuum – Deadly Force
  - Used as last resort when all other means have failed or use of deadly force is justified

9

Strategies

- Four strategies for interruption and neutralization
  - **Denial** – preventing adversaries from getting to an asset
  - **Containment** – preventing adversaries from leaving the site with an asset
  - **Recapture** – taking over by force a critical location on the site occupied by adversaries
  - **Pursuit and Recovery** (contingency) – attempting to recover an asset removed from the site by adversaries

10

Aspects of Response

- Deployment of response personnel
- Communication with response personnel

11

Deployment of the Response Force

- Deployment is the action of initiating personnel response to confront the adversary and requires Planning, Training, and Practice
- Response Force Equipment
  - Weapons – non-lethal and lethal
  - Personnel survivability– body armor, gas masks, chemical/biological suits, armored vehicles, fighting positions
  - Miscellaneous – night vision , flashlights, hand cuffs, load-bearing vest
  - Communication Equipment

12

Communication with Response Personnel

- Vital to command and control
  - Situational awareness
  - Duress

- Multiple mechanisms for operations and contingency
  - Pagers
  - Phones – cell or land lines
  - Sirens and lights
  - Intercoms and public address systems
  - Computer terminals
  - Duress systems

13

Roles for Response

- Training –
  - General use of equipment – weapons, gear, communication systems and AC&D system
  - Scenario-based – Guards and Response Forces for normal operations and contingency missions, understand tactics
  - Sustained and dynamic – maintains awareness of conditions and changes and proficiency
  - Performance based testing force-on-force exercises

14

Role of Command, Control, and Communication

- **Command:** Exercise of authority (decision making) by response force leaders
- **Control:** Direction by Response Force leaders over assigned personnel to accomplish the mission
- **Communications:** Allow real-time communication between the central alarm station, tactical leaders, and Response Force in the field and allow tactical leaders to direct the actions of the response based on adversary actions

15

Decisions to be made:

- Use of force
- Rules of engagement
- Guards versus response force responsibilities
- Types of communication
- Weapon systems and equipment
- Training
- Meets the DBT

Summary

- Response follows Detection and occurs in parallel with Delay.
- Guard Forces perform routine, on-site duties and Response Forces are responsible for interruption or neutralization of an adversary.
- The levels of force – use-of-force continuum ranges from presence to deadly force.
- The four strategies for interruption and neutralization are denial, containment, recapture, and pursuit and recovery.
- Communication is vital to command and control
  - Command – authority of response force leaders
  - Control – direction by response force leaders to response force
  - Communication – allows leaders to direct actions of the response based on adversary actions
- General Considerations of response functions are tactical Planning, Training, and Practice.

17

Conclusion

Questions before we continue?

18

This page intentionally left blank.

Infrastructure Development: Initiating a Physical Protection Program

Module 14:
System Effectiveness Evaluation

1

Module Objectives

After completing this module you should be able to do the following:

- Recognize the requirement for evaluation
- Describe the evaluation approaches
- Identify evaluation tools
- Describe two major factors that determine the quality of PPS performance evaluation

2

Relationship to INCIRC/225/Rev 5

- *4.4.2.4. To ensure that physical protection measures are maintained in a condition capable of meeting the State's regulations and of effectively responding to the State's requirements for physical protection, the State's competent authority should ensure that evaluations based on performance testing are conducted by operators at nuclear facilities and by shippers or carriers for transport. Evaluations should be reviewed by the State's competent authority, and should include administrative and technical measures, such as testing of detection, assessment and communications systems, and reviews of the implementation of physical protection procedures. When deficiencies are identified, the competent authority should ensure that corrective action is taken by the operator and by the shipper or carrier.*

3

Evaluation Objectives

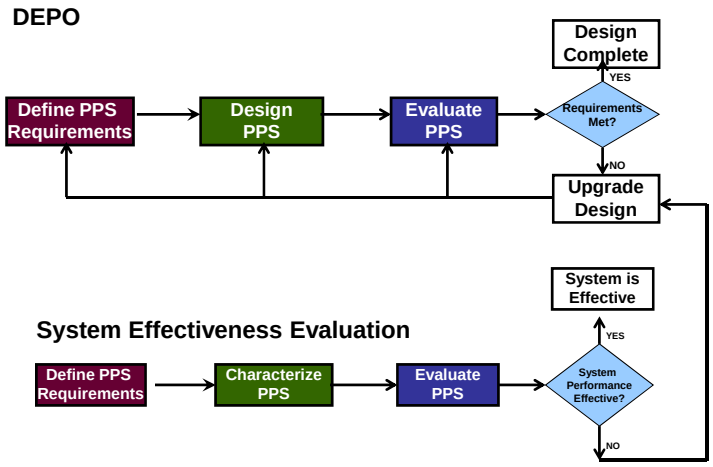
The Competent Authority and Licensees have complementary objectives for the evaluation of PPS:

- Meet regulatory and licensee requirements
  - Self-assessment by licensee
  - Inspection by competent authority
  - Periodic re-validation
- Verify and/or improve PPS performance
  - Verify PPS satisfies requirements
  - Identify system deficiencies
  - Analyze system upgrades
  - Compare cost versus performance
  - Select/implement overall best option

4

4

Design and Implementation Evaluation



5

Evaluation Approaches

- ***Expert:*** Performs PPS design and evaluation activities relying on personal knowledge and experience
- ***Prescriptive Approach:*** PPS design and evaluation based on specification and implementation of a required set of features
- ***Component Criteria Approach:*** standards approach to PPS design and evaluation that uses performance criteria for some security features
- ***System Performance Approach:*** A systems engineering approach to the design and evaluation of PPS based on specifying and achieving an overall system effectiveness against the Design Basis Threat (DBT) for theft and sabotage

6

Discussion on Evaluation: New Sensor Case Study (1 of 4)

You have been approached by a vendor regarding a new type of sensor to consider for your physical protection system.

- How do you decide whether to use the sensor or not in your design?
- How do you understand the impacts to your existing system?

7

Discussion: New Sensor Case Study (2 of 4)

- Expert-based approach: a security expert might tell you in their opinion that it is desirable to have the sensor
  - How would you validate that opinion?
- Prescriptive approach: Requirement for a particular sensor type
  - Is this sensor part of the allowed sensor type?
  - How does the sensor perform in your particular environment?
  - What impacts does this sensor type have on the overall system performance?

8

Discussion: New Sensor Case Study (3 of 4)

- Component criteria approach: In this approach, there is a requirement to include required features that meet specific performance standard,
  - Example: “Probability of detection greater at the perimeter must be greater than 0.95 with a false alarm rate less than 1 in 10,000 alarms
  - How would you determine that sensor truly has that performance?
  - How would you know the impact of the sensor on the system performance?

9

Discussion: New Sensor Case Study (4 of 4)

- A system performance approach: Considers several issues in a disciplined approach:
  - Requirements:
    - What assets need protecting?
    - Who do these targets need to be protected from?
    - What level of protection is needed to protect the targets?
    - Are there reasons not to use the sensor?
  - Characterizing the PPS
  - Evaluating effectiveness
- How do you answer the “buy or don’t buy” question?
- How do you validate your answer with the results of the analysis?

10

Performance-based Approach

Recall, from the risk management and regulatory requirements module, the performance approach:

- The Competent Authority specifies the required level of system effectiveness, probability of effectiveness, against the DBT for the Licensee
- The Licensee complies by designing and evaluating its physical protection system to achieve this probability of effectiveness
- The Competent Authority is responsible for verifying that the Licensee's system satisfies the required performance against the potential adversary

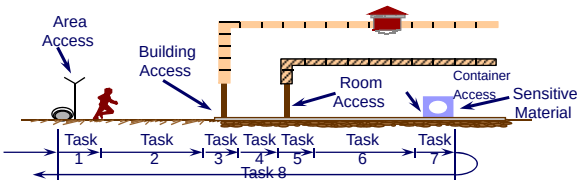
11

Evaluation Tools

- Path Analysis – single/multipath
- Adversary Sequence Diagrams
- Scenario-based Analysis
- Exercises
  - Modeling/Simulation
  - Table Top
  - Force-on-Force

Adversary Sequence Diagram

Adversary Path: A time-ordered sequence of path elements, areas, and a target task that the adversary must traverse to complete an attack

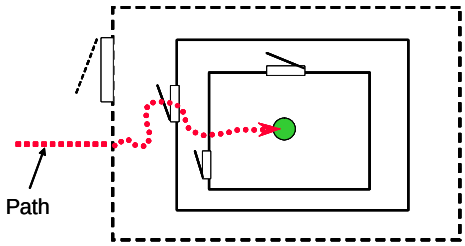


Metric – Total adversary task time

13

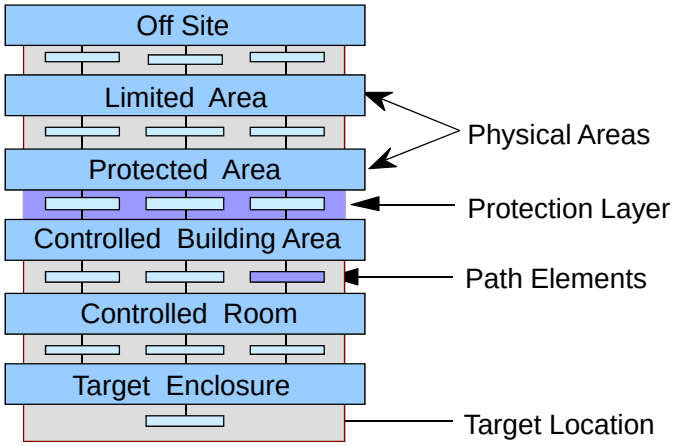
Concept of an Adversary Path

Path Analysis: An analysis using time-ordered sequence of path elements that examines the probability of detection and adversary task delay against the response force time



14

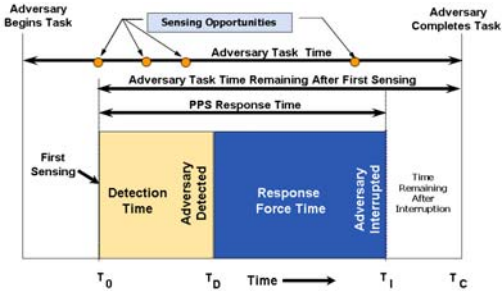
Concept of Adversary Sequence Diagram



15

Path Analysis Uses Two Concepts

- Adversary and PPS Timelines, discussed in the Design module, are used to calculate probability of interruption:

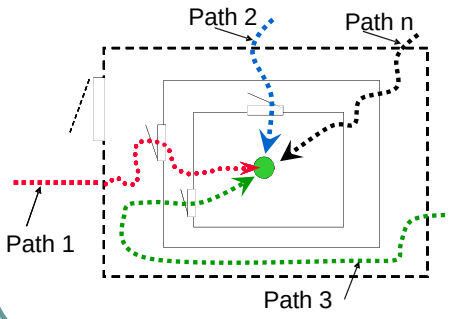


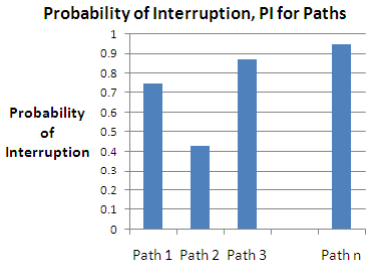
Metric: Probability of Interruption

16

Multi-path Analysis

Multi-path analysis: determines whether detection and delay are sufficient along all adversary paths to provide an adequate level of Probability of Interruption, P_I, based on planned PPS Response Times

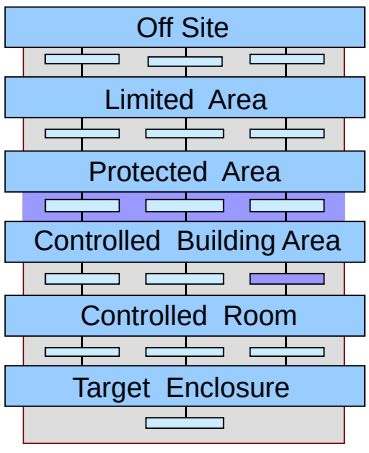




17

17

Developing a Scenario from a Path



Adversary Activities (Four adversaries)
Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during storm, last adversary monitors radio traffic.
Two adversaries penetrate door using burn bar, avoid sensor activation.
Two adversaries penetrate wall using linear shaped charge at night during storm.
Two adversaries destroy pump with linear shaped charge. All adversaries retreat.

18

Details of Scenario

Adversary	System	Response Force
Three adversaries drive up to gate in truck act as lost.	**Normal procedures followed**	**Random Patrol in effect**
Two adversaries surreptitiously generate a fence alarm then lie in wait to ambush patrol.		**Unassessed alarm reported to patrol**
The two teams coordinate an attack on the patrol and gatehouse.		**Random Patrol ambushed near perimeter P_N=0.2** **Gatehouse guards attacked P_N=0.3**
The team of three set up ambush for secondary responders.		**Secondary responder mobilize** **Secondary responders are ambushed probability of neutralization 0.50**
Remaining adversaries proceed to storage vault and remove material.	**Sensor's alarm**	**No forces available to respond**

19

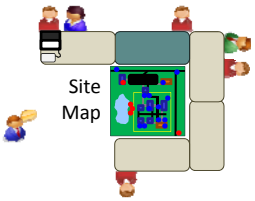
Scenario Evaluation

- System effectiveness is estimated considering the detection and delay at each of the scenario steps and the effectiveness of the response
- The team's expert opinion will be based on
  - Likelihood of detection achieved by the system
  - Duration of delay (after detection) being long enough for response to be effective
  - Ability of response to stop the adversary from achieving their goal if the response arrives in time

20

Exercises

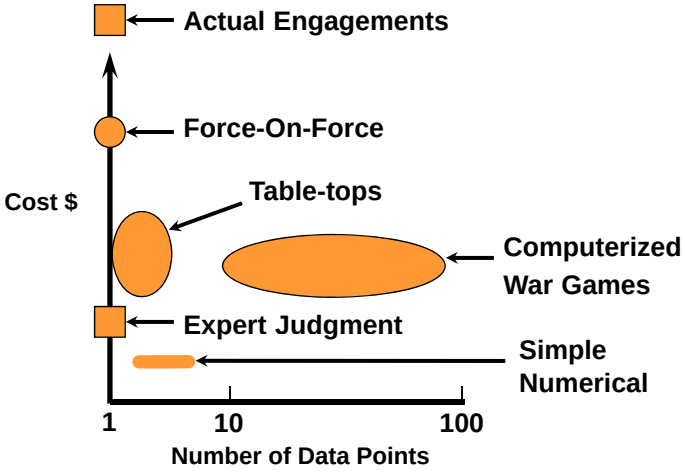
- Computer Combat Simulation Methodology
- Force-on-Force (FoF) Exercise Methodology (good at replicating individual behaviors)
- Tabletop Exercise Methodology (good at replicating decision-making)



Metric:
Probability of Neutralization

21

Probability of Neutralization Cost



22

Evaluation Quality

- There are two major factors that determine the quality of the PPS performance evaluation:
  - Subject matter experts
    - Subject matter experts and their expert knowledge and experience are involved in the application of all evaluation methodologies
  - Performance test data
    - Security component (detection, delay, and response) performance data used in the system evaluation must be high quality
    - Component performance data should be based on current performance testing

23

23

Decisions to be made

- Performance Criteria
- How to prove that system meets the criteria
- Evaluation approach
- Tools that will be used to validate performance
- Quality of evaluation

24

Summary

- INFCIRC/225/Rev 5 requires performance-based evaluation of physical protection systems
- Systems may be evaluated using expert, proscriptive, component, or system effectiveness approaches
- Evaluation tools include:
  - Adversary Sequence Diagrams
  - Path Analysis – single/multipath
  - Scenario-based Analysis
  - Exercises - Modeling/Simulation, Table Top, Force-on-Force
- Two major factors affecting evaluation quality are:
  - Subject matter experts and performance test data

25

25

Conclusion

Questions before we continue?

26

Infrastructure Development: Initiating a Physical Protection Program

Module 15:
Transportation Security

1

Module Objectives

After completing this module, you should be able to do the following:

- Compare similarities and differences between fixed-site and transportation security
- Identify protection actions that can be taken
- Recognize the decisions to be made regarding transportation of nuclear and other radioactive materials

2

Transportation Elements

- Material movement within a site
- Material movement to and from a site

Spent-Fuel Cask on Rail Car

3

Differences

Fixed-Site	versus	Transport
Fixed Protection Boundary		Moving Boundary
Stable Environment		Continuously Changing
Control Over Environment		Uncontrolled Environment
Operations are Predictable		Variation in Schedule
Protection System in Place		Protection System must be Transportable

4

Differences

- Requires scenario analysis instead of a path analysis
  - Travel through public areas with no protected area
  - Constantly changing surroundings
  - Adversary attack and first detection both begin at the target

5

Similarities

- Follows the same design and evaluation process as for a fixed site
  - Determine system objectives
  - Characterize existing system or design a new system
    - Detection / Delay / Response
  - Analyze PPS

6

Transportation Conveyances

7

Transportation Threat Examples

8

Transportation Detection, Assessment, Communication

- Detection
  - Outsider
    - Interior alarms
    - Response forces
  - Insider
    - Access control, includes 2-person rule
- Assessment and communications
  - Response force communicates alarm
  - Response force performs visual assessment

9

Delay Considerations

What makes working on
your car time-consuming or difficult?

10

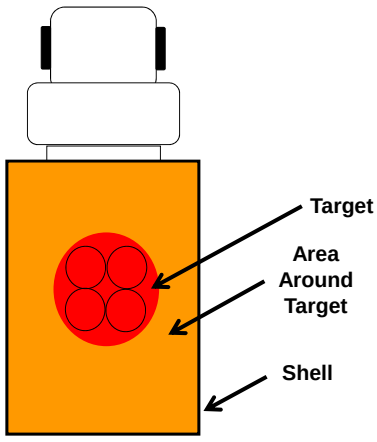
Transportation Delay Principles

- Transportation delay principles provide:
  - Concealed delay features
  - Keeping cargo secured to vehicle
  - Forcing adversary to perform sequential tasks to gain access
  - Forcing adversary to use many different tools to defeat delay features
  - Creating difficult work area for the adversary
  - Balanced delay

11

Delay Techniques

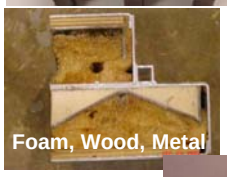
- **Delay Techniques**
  - **Hardened vehicle**
  - **Interior hardening**
  - **Delay at asset**
- **Examples**
  - **Transporter**
  - **Doors and locks**
  - **Cages and tie-downs**
  - **Activated barriers**



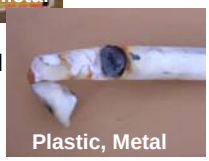
12

Example of a Transporter

Ballistics Protection

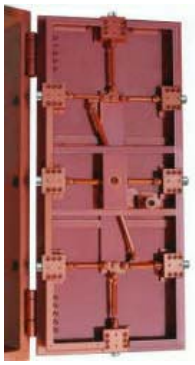


Multi-Layered Barriers



13

Doors and Locks



Hardened Doors

Electric Lock

Internal Lock

Shrouded Lock

14

Cages and Tie-Downs

15

Activated Barriers May Be Applied

- Exert minimum impact on operations
- Afford volume protection
- Must provide adequate safety to personnel
- Offer multiple activation options

Rigid Polyurethane Foam

16

Transportation Access Delay Considerations

- Constraints
  - Vehicle size and weight
  - Operational requirements
  - Standard vehicles provide minimal delay
- Delay Principles
  - Balance delay for all surfaces and all attacks
  - Use concealed delay features
- Adversary
  - Force adversary to perform sequential operations
  - Minimize adversary work area
  - Create difficult working environment for adversary
- Response
  - Consider insider issues in the design, use 2-person control
  - Need enough delay for response force to win
- Access delay features should be present 100 % of the time or take compensatory measures

17

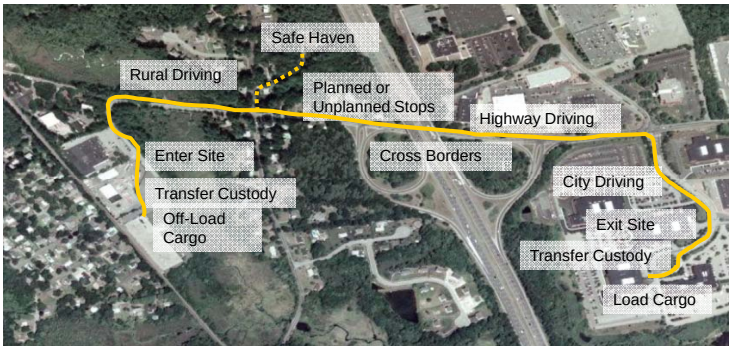
Transportation Response

- Response force numbers, equipment, and training required depends on the threat
- Communications to
  - Each member of the response force
  - Secondary response force members
  - Transport control station
- Response Force configuration
  - Number of responders and their location relative to target
  - Secondary response force

18

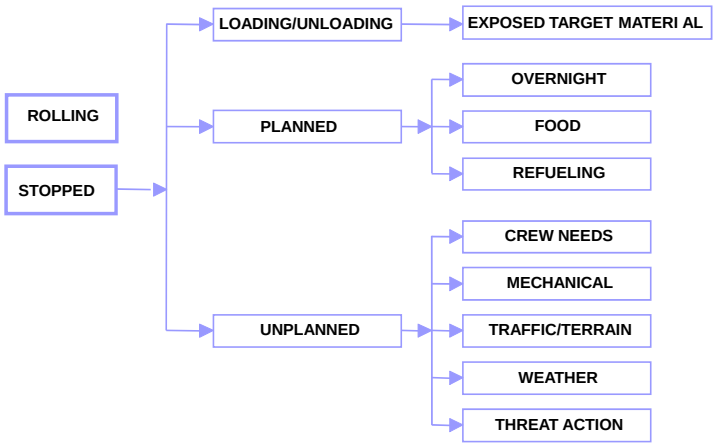
Transportation Analysis

- Scenario analysis is most common tool
  - Vehicle states
  - Route surveys
- The scenario should be simple to carry out and consistent with the adversary's capabilities



19

Vehicle States



20

Possible Protection Actions

- Increase delay
- Enhance response force capabilities
- Vary routes and times
- Change location for scheduled stops
- Use look-alike shipments or decoys
- Dispatch covert shipments
- Use of high-profile shipments (military escort) or low-profile (civilian look-alike)
- Perform route surveillance reviews

21

Decisions to Be Made

- Processes for chain of custody
- Mode of transport
- Siting and routing transportation considerations
- Role and type of response

22

Summary

- There are both similarities and differences between fixed-site and transportation security
- Protection actions that can be taken include conveyance design, varied routing, and decoys
- Decisions to be made regarding transportation of nuclear and other radioactive materials
  - Mode of transport
  - Siting and Routing
  - Response

23

Conclusion

Questions before we continue?

24

This page intentionally left blank.

Infrastructure Development: Initiating a Physical Protection Program

Module 16:

Summary of Decisions to Be Made

1

Module Objective

- At the end of this module, you should be able to identify the decisions that need to be made to initiate a Physical Protection Program

2

Nuclear Security Program Topics Covered

- Legal Framework
- Regulatory Framework
- Nuclear Security Programs
  - Physical Protection Program
  - Material Control and Accounting
  - Information Security
  - Personnel Security
- Physical Protection Systems
  - Requirements
  - Elements
  - Evaluation
- Transportation Security

3

Legal Framework Decisions - State

- Participation in international agreements
  - IAEA, NPT, Additional Protocol
  - Convention of the Physical Protection of Nuclear Material
  - Security Council Resolutions 1540 and 1373
  - International Convention for the Suppression of Act of Nuclear Terrorism
  - Code of Conduct on Safety and Security of Radioactive Sources
  - Guidance on the Import and Export of Radioactive Sources
- Designation of government agency(s) will be responsible for regulation of the physical protection for nuclear and radioactive materials and for working with the legislative body
- Identification of what nuclear and radioactive materials are permitted
- Identification of agency assigned to perform an intelligence-based threat assessment and determination on who how decisions will be made based on this threat assessment
- Select mechanisms for security transport of nuclear and other radioactive materials
- Response force responsibility and authorities

Regulatory Framework Decisions

- Develop a regulatory approach
  - Prescriptive
  - Performance
- Establish regulatory framework covering:
  - Licensing and evaluation of continued compliance
  - Definitions
  - Requirements
  - Considerations
  - Design Basis Threat
- Graded approach framework
  - Material categorization
  - Classification levels for the protection of information and materials
  - Levels of personnel trustworthiness

Nuclear Security Program Regulatory Decisions

- Physical Protection System
  - Define design and evaluation process
  - Evaluation criteria
- Material Control And Accounting
  - Determine material accounting system
  - Identify system requirements for material control
- Information Security
  - Determine process of certification and continued accreditation of information system
- Personnel Security
  - Identify a personnel identification system
  - Determine access and privileges levels

Licensee Physical Protection System Requirements Decisions

- What needs to be protected?
  - Targets and target locations
- What threats to protect against?
  - DBT and local threat information
- What level of protection is adequate?
  - Performance criteria
  - Evaluation processes and tools

Licensee Physical Protection System Design Decisions

- Facility Siting
- Security areas and layers of protection
- Detection and assessment for each layer of protection
- Access control system for each layer of protection
- Delay mechanisms for each layer of protection
- Guard/response force capabilities

Facility Siting

Location Considerations

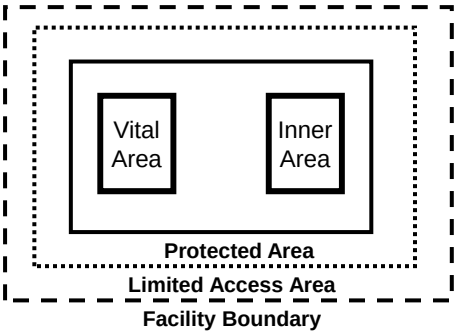
- Population centers
- Nearby businesses/structures
- Nearest emergency response group
- Security response force location
- Availability and reliability of power and communications
- Proximity to labor pool
- Local crime
- Wide-open spaces

Environment Considerations

- Topography at the site
- Vegetation and wildlife
- Background noise
- Climate and weather
- Soil conditions
- Water flows/drainage

Protection Layers and Associated Security Areas

- Typical Layers:
  - Limited access area
  - Protected area
  - Inner area
  - Vital area



- Some protection systems may have more or fewer areas.

10

Detection and Assessment Decisions

- Detection system requirements – exterior/interior
- Covert versus visible detection
- Assessment using technology or manpower
- Complexity of the alarm monitoring station
- Alarm prioritization
- Alarm control and display system requirements
- Adequate infrastructure to support detection and assessment systems
- Performance test requirements
- Sustainability

Access Control Decisions

- Minimum number of access points for each protection layer
- Type of access control to be employed – technology, manpower, combination
- Adequate infrastructure to support access control
- Emergency situation management
- The need for contraband detection (entry/exit)
- Contraband materials list

Delay Decisions

- On-site or off-site response determines the delay necessary
- Passive or activated barriers

Response Decisions

- Location of forces – onsite/offsite, stations
- Use of force
- Rules of engagement
- Guards versus response force responsibilities
- Types of communication
- Weapon systems and equipment
- Training
- Levels needed to meets the DBT

System Evaluation Decisions

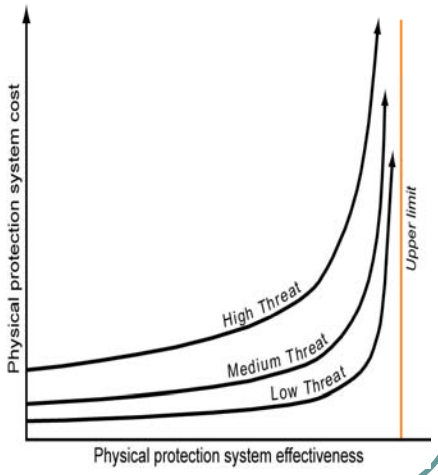
- Performance Criteria
  - How to prove that system meets the criteria
- Evaluation approach
  - Tools that will be used to validate performance
- Quality of evaluation

Transportation Decisions

- Processes for chain of custody
- Mode of transport
- Siting and routing transportation considerations
- Role and type of response

Cost vs. System Effectiveness Decisions

- Decisions that need to be made:
  - Siting
  - Design of PPS
    - Detection
    - Delay
    - Response
- Cost trade-off



17

Summary

- There are many decisions that must be made when designing a physical protection system for nuclear security applications for
  - Fixed Sites
  - Transportation

Infrastructure Development: Initiating a Physical Protection Program

Module 17:
Next Steps for Collaboration

1

Module Objective

- Summarize material covered
- Discuss future collaboration
- Determine next steps

2

Topics Covered

- Nuclear Security Legal Framework
- Supporting Regulatory Framework
- Physical Protection Systems
- Personnel Security
- Information Security
- Transportation Security

3

Opportunities for Bilateral Collaboration

- Physical Protection Exchange Visits
- Site Assessments
- Technical Guidance
- Professional Training
- Best Practices Working Group

4

Professional Training

- Regional or national training courses on
  - Physical Protection of Nuclear Material and Nuclear Facilities
  - Security of Research Reactors
  - Foundations of Physical Protection
  - Design Basis Threat (DBT)
  - Protection against Sabotage
  - Vital Area Identification
  - Insider Threat
  - Nuclear Security Culture
  - Initiating a Physical Protection System Practical 5-Day Course

5

Next Steps

- What types of collaboration would you like to pursue?
- Who would be the point of contact?
- What would be the venue?
- What access would be required?

6

Summary

- This was only an introduction to physical protection.
- States must provide a legal and regulatory framework for physical protection.
- Every element of physical protection has effectiveness versus cost trade-offs.

7

Thank You!

- We appreciate your participation in this workshop.
- Your feedback is welcome and needed.
- We look forward to future collaboration.

8

Infrastructure Development: Initiating a Physical Protection Program

Student Workbook

June 2010 Edition
Part 1

Table of Contents

Module 1
Introduction and Overview

Introductions

- Workshop Director -
- NNSA Representative -
- Instructors -

Please introduce yourself to the class

- Name
- Organization and job
- Nuclear security experience
- What you expect to get from this workshop

Workshop Schedule

- **Day 1**
  - Introduction
  - Nuclear Security Regime
- **Day 2**
  - Physical Protection Systems
- **Day 3**
  - Transportation Security
  - Physical Protection Decisions to Be Made
  - Next Steps in Collaboration
  - Closing

Process of the Workshop

- This is an overview course to provide awareness of roles and elements of a physical protection program

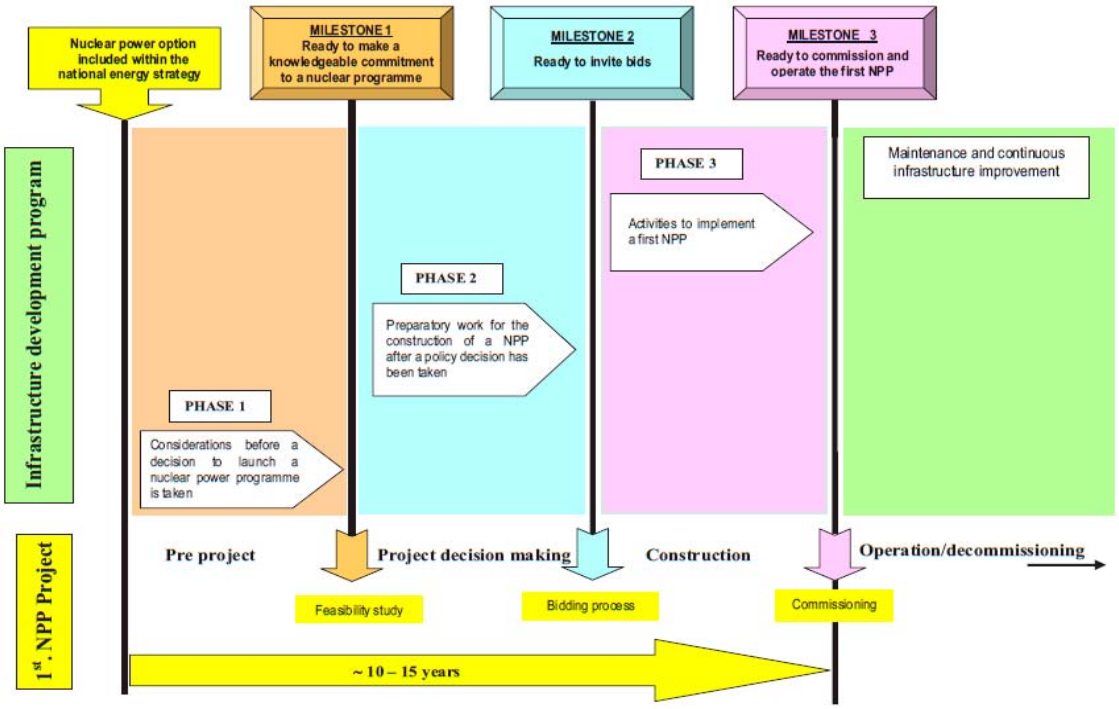
- Opportunities for further collaboration on developing or enhancing a nuclear security program will be discussed

Workshop Objectives

1. Define the legal and regulatory frameworks needed to support Physical Protection
2. Identify the functions and elements of a Physical Protection Program
3. Recognize the decisions that need to be made to implement Physical Protection Systems

Module 1
Nuclear Security Overview

The Infrastructure Development Model provides an overview of the entire program to develop the national infrastructure for nuclear power. This Model is taken from the International Atomic Energy Agency (IAEA) Nuclear Energy Series NG-G-3.1 and shows the various phases of a Nuclear Energy Infrastructure Development Program.



The activities are split into three progressive phases of development. The completion of the work at each of these phases is marked by a specific milestone at which the progress and success of the development effort can be evaluated and a decision made to move on to the next phase.

Phase 1 – Considerations before a decision to launch a nuclear power program is taken
Phase 2 – Preparatory work for construction of a nuclear power program after a policy decision has been made
Phase 3 – Activities to implement a Nuclear Power Program
Phase 4 – Maintenance and continuous infrastructure improvement

It is necessary to understand the purpose of the evaluation of each phase. For phase 1, the evaluation concerns the quality of information available and the effective investment of resources for informed decisions and the management of program risk. While a Member State can do less work in phase 1, there is a much greater risk of an ill informed decision, or of phase 2 taking much longer than planned because the necessary issues have not been properly researched.

There are 19 infrastructure issues that have requirements to meet the three milestones associated with the first three phases.

TABLE 1. INFRASTRUCTURE ISSUES AND MILESTONES

Issues	Milestone 1	Milestone 2	Milestone 3
National position			
Nuclear safety			
Management			
Funding and financing	CONDITIONS	CONDITIONS	CONDITIONS
Legislative framework			
Safeguards			
Regulatory framework			
Radiation protection			
Electrical grid			
Human resources development			
Stakeholder involvement			
Site and supporting facilities			
Environmental protection			
Emergency planning			
Security and physical protection			
Nuclear fuel cycle			
Radioactive waste			
Industrial involvement			
Procurement			

Security and Physical Protection Milestones

Milestone 1 – Ready to make a knowledgeable commitment to a nuclear program

- Requirements for security and physical protection acknowledged
- Necessary legislation identified

Milestone 2 – Ready to invite bids for the first nuclear power plant

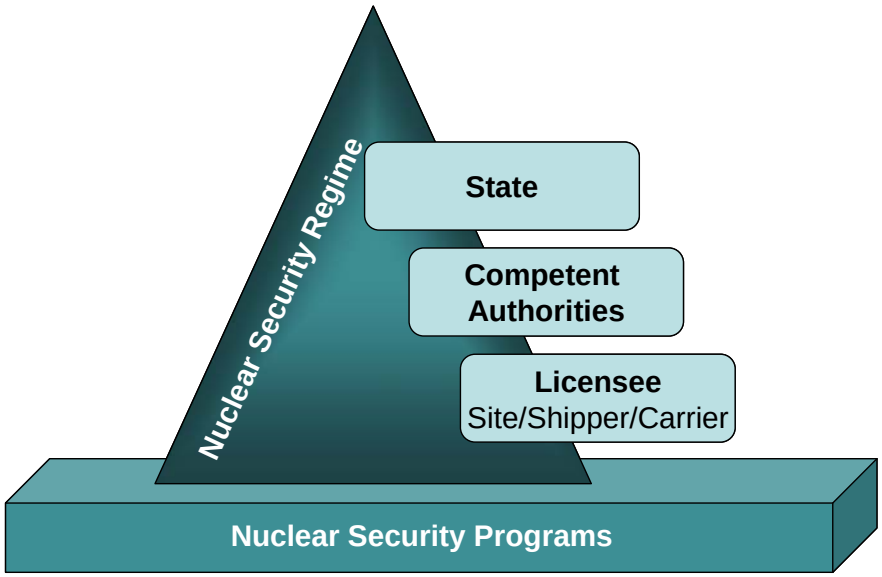
- Legislation promulgated
- DBT defined
- Security requirements defined

- Sensitive information defined
- Physical protection by trained on-site security staff provided
- Local and national law enforcement assistance established
- Programs for selection/qualification of staff accessing to facilities or sensitive information are in place

Milestone 3 – Ready to commission and operate the first nuclear power plant

- All security conditions established and implemented

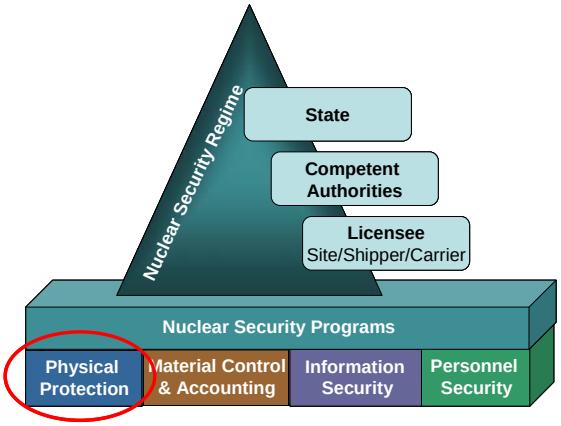
This translates into development of a State's Nuclear Security Regime. Based on the guidance provided from the IAEA there are there are three main entities associated with the Nuclear Security Regime.



The **State** (a country's governing body) is ultimately responsible for the security of nuclear and radioactive materials. The state establishes the legal framework and designates one or more competent authorities the responsibility for the regulatory and licensing framework.

These **competent authorities** work together with the licensees to meet the State's obligations for nuclear and other radioactive materials.

The **licensees** may be facility operators at sites or shippers/carriers of nuclear and other radioactive materials. Note that licensees may be either public entities or private businesses



Physical Protection is part of a State's Nuclear Security Regime

PHYSICAL PROTECTION REGIME: A regime including:

- the legislative and regulatory framework governing the physical protection of *nuclear material, nuclear facilities,* and other radioactive materials and associated facilities;
- the institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework; and
- facility-level and activity-level *physical protection systems.*

PHYSICAL PROTECTION PROGRAM: The combination of the physical protection system policies, procedures, and physical protection systems

PHYSICAL PROTECTION SYSTEM: An integrated set of *physical protection measures* intended to prevent the completion of a *malicious act*.

Nuclear and Radioactive Material

Benefits

- Nuclear
  - Generation of high amounts of carbon-free electrical energy
  - Low carbon dioxide emissions
  - Existing technology
- Radioactive Materials
  - Medical
  - Industry
  - Food Safety

Risks

- Accidents
- Target for attack
- Radioactive waste

Significant Potential Risks Associated with Nuclear Materials

- Theft
    - Material for an improvised nuclear device
    - Material for a radiation dispersion device

- Sabotage
    - Loss of functionality
    - Dispersion of radioactive material

Outline for this Course

- NNSA International Protection Program
- Legal Framework
- Regulatory Framework
- Overview of Nuclear Security Program
- Overview of Physical Protection System (PPS)
    - Requirements Definition, Design Basis Threat, and Targets
    - Characterization and Siting Impacts
    - Elements of PPS Design Detection, Delay, and Response
    - Physical Protection Systems Evaluation
- Transportation Security
- Decisions to be Made
- Next Steps in Collaboration

Summary

- Nuclear and other radioactive materials can provide great benefit, but can generate significant risks

- PHYSICAL PROTECTION SYSTEM: An integrated set of *physical protection measures* intended to prevent the completion of a *malicious act*

Module 2
NNSA International
Physical Protection Program

Module Objectives

- Define Program Scope
- Discuss Program Activity Areas
    - Site Assessments
    - Technical Guidance
    - Professional Training
    - Bilateral Collaboration
- Identify Program Management Tools

Need for Physical Protection and IPP Role

The need to protect nuclear material and facilities globally is imperative; terrorists have demonstrated their willingness to inflict mass causalities and have announced their intention to acquire nuclear material.

The NNSA Office of Nuclear Safeguards and Security (NA-241) works to ensure physical protection of nuclear material and facilities by:

- Bilateral physical protection visits
- Development and support of international nuclear security policy and guidance
- Training of personnel responsible for protecting nuclear material
- Bilateral technical collaboration

NA-241 cooperates with other U.S. Organizations and the IAEA for collaboration on physical protection:

- National Nuclear Security Administration
    - Office of Defense Nuclear Security
    - Office of Global Threat Reduction
    - Office of International Material Protection & Cooperation
- Department of Energy's Office of Counter Terrorism
- Department of State
- Nuclear Regulatory Commission
- Defense Threat Reduction Agency
- Sandia and other U.S. National Laboratories
- International Atomic Energy Agency (IAEA)

Program Scope

- Physical protection of nuclear material during use, storage, and transport
- U.S.-obligated nuclear material in countries with bilateral agreements
- IAEA Office of Nuclear Security and Member States
- Bilateral collaboration with non-weapon states
- Excluding implementation of upgrades
- Site Assessments
    - Countries with U.S.-obligated nuclear material (approx. 50)
    - Physical protection obligation specified in “123” Agreement
    - Based on international norm of IAEA INFCIRC/225
    - Compliance required for exports
    - Physical protection exchange visits
    - Assessment is not an inspection

Bilateral Physical Protection Visits to 46 countries

Argentina	Finland	Luxembourg	Slovenia
Australia	France	Malaysia	South Africa
Austria	Germany	Mexico	Spain
Belgium	Greece	Morocco	Sweden
Brazil	Hungary	Netherlands	Switzerland
Bulgaria	India	Norway	Thailand
Canada	Indonesia	Pakistan	Turkey
Chile	Ireland	Paraguay	United Kingdom
Columbia	Israel	Peru	Uruguay
Czech Republic	Italy	Philippines	Venezuela
Denmark	Japan	Portugal	Yugoslavia
	Korea	Romania	

Technical Guidance (NA-241/SNL support)

- IAEA Nuclear Security Series
    - Fundamentals
    - Recommendations
    - Implementing Guides
    - Technical Guidance
- Process
    - Document Preparation
    - Consultancy Meetings
    - Technical Meetings

IPP Assistance with NSS Publications

<u>Published</u>

- Protection against an Insider Threat
- Nuclear Security Culture

<u>In Development</u>

- Development of Design Basis Threat
- Identification of Vital Areas
- Protection against Sabotage
- Nuclear security fundamentals
- Protection of nuclear material and facilities (INFCIRC/225/Rev.5)

Professional Training

- Original U.S. commitment in Nuclear Nonproliferation Act of 1978
- International Training Course (ITC) on Physical Protection of Nuclear Facilities and Materials
    - Over 600 participants from 60 countries
    - Lectures, subgroup exercises, field activities, and final comprehensive exercise using hypothetical facility
    - Taught by SNL in ABQ, 3 weeks, in English
    - ITC-21 completed in May 2009
- IAEA courses developed and presented via NA243/SNL process
    - Regional/National Training Course on Physical Protection of Nuclear Material and Nuclear Facilities
    - Regional/National Training Course on Security of Research Reactors
    - Regional/National Training Course on Foundations of Physical Protection
    - Design Basis Threat
    - Protection against Sabotage
    - Vital Area Identification
    - Insider Threat
    - Nuclear Security Culture

Bilateral Collaboration

- Based on U.S. nuclear material security interests to:
    - Enhance international nuclear security
    - U.S. intellectual gain
- Recent and current partners
    - Japan
    - Republic of Korea
    - France
    - Brazil
    - Argentina

Summary

- Program scope includes physical protection of nuclear material, U.S.-obligated nuclear material, IAEA Office of Nuclear Security and Member States, bilateral collaboration
- Program activity areas include:
    - Site Assessments
    - Technical Guidance
    - Professional Training
    - Bilateral Collaboration
    - A variety of Program Management Tools are used to monitor program activities

Module 3
Legal Framework

Module Objectives

- Introduce the legal responsibilities of the State for the security of nuclear and other radioactive material
- Recognize decisions that need to be made at the State level

International Legal Instruments for Physical Protection

- Nuclear Materials
  - Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment
  - The Physical Protection of Nuclear Materials and Nuclear Facilities, INFCIRC/225/Rev.4 (corrected)
- Other Radioactive Materials
  - Code of Conduct on the Safety and Security of Radioactive Sources
  - Guidance on the Import and Export of Radioactive Sources
- Convention on the Suppression of Acts of Nuclear Terrorism
- UN Security Council resolutions 1373 (2001) and 1540 (2004)
- Safeguards agreements and their additional protocols

Convention on the Physical Protection of Nuclear Material (CPPNM)

- Defines what is “nuclear material”
  - plutonium except that with isotopic concentration exceeding 80% in plutonium-238; uranium-233; uranium enriched in the isotope 235 or 233; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore-residue

- Identifies State’s Responsibilities
  - Each State Party shall take appropriate steps within the framework of its national law and consistent with international law to ensure nuclear material is protected at the levels commensurate with the type of material

CPPNM – Legal Responsibilities

- Controlled import/export of nuclear materials
- Security of nuclear materials while in transit within and across the State, by land, water, and air
- Designation of central or competent authority for the physical protection of nuclear material and coordinating recovery and response operations
- Protection of the confidentiality of information
- Criminal penalties

CPPNM Criminal Penalties - The intentional commission of:

- an act without lawful authority which constitutes the receipt, possession, use, transfer, alteration, disposal or dispersal of nuclear material and which causes or is likely to cause death or serious injury to any person or substantial damage to property;
- a theft or robbery of nuclear material;
- an embezzlement or fraudulent obtaining of nuclear material;
- an act constituting a demand for nuclear material by threat or use of force or by any other form of intimidation;
- a threat:
    - to use nuclear material to cause death or serious injury to any person or substantial property damage, or
    - to commit an offence in order to compel a natural or legal person, international organization or State to do or to refrain from doing any act;
- an attempt to commit or participate in any offence listed above

CPPNM Amendment

- Explicitly includes nuclear material and *nuclear facilities*
- Added sabotage considerations
- The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State Party rests entirely with that State.
    - Establish and maintain a legislative and regulatory framework to govern physical protection;
    - Establish or designate a competent authority or authorities responsible for the implementation of the legislative and regulatory framework; and
    - Take other appropriate measures necessary for the physical protection of nuclear material and nuclear facilities.
- Adds the 12 Fundamental Principles for Physical Protection of nuclear material and nuclear facilities

12 Physical Protection Fundamental Principles

1. Responsibility of the State
2. Responsibilities during international transport
3. Legislative and regulatory framework
4. Competent authority
5. Responsibility of the license holders
6. Security culture
7. Threat
8. Graded approach
9. Defense-in-depth
10. Quality assurance
11. Contingency plans
12. Confidentiality

CPPNM Amendment (continued)

Each State Party shall establish, implement and maintain an appropriate physical protection regime applicable to nuclear material and nuclear facilities under its jurisdiction, with the aim of:

(a) protecting against theft and other unlawful taking of nuclear material in use, storage and transport;

(b) ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material; when the material is located outside its territory, that State Party shall act in accordance with article 5;

(c) protecting nuclear material and nuclear facilities against sabotage; and

(d) mitigating or minimizing the radiological consequences of sabotage

CPPNM – Extended Criminal Penalties

1. Add the environment to impacts of malicious acts
2. Added robbery, embezzlement, and fraudulent obtaining of nuclear material
3. Added an act which constitutes the carrying, sending, or moving of nuclear material into or out
4. of a State without lawful authority;
5. Extended the range of criminal actions to
    - Demanding nuclear material by threat or use of force or by any other form of intimidation;
    - Threatening to use nuclear material to cause death or serious injury to any person or substantial damage to property or to the environment
    - Planning, attempt, threat of, commission, participation in malicious acts using nuclear material or against nuclear facilities

Questions

A. Is your country a signatory to CPPNM?_____
B. To its Amendment?_____

INFCIRC 225/Rev 5 – The Physical Protection of Nuclear Material and Nuclear Facilities

- Objectives of a State's Physical Protection Regime
- Elements of a State's Physical Protection Regime for Nuclear Material and Nuclear Facilities
- Requirements for Measures Against
    - Unauthorized Removal of Nuclear Material in Use and Storage
    - Sabotage of Nuclear Facilities and Nuclear Material in Use and Storage
    - Unauthorized Removal and Sabotage of Nuclear Material During Transport

INFCIRC 225/Rev 5 – Legislative Framework Requirements

A State should

- Take appropriate measures within the framework of its national law to establish and ensure the proper implementation of the State's physical protection regime.
- Define requirements for the physical protection of nuclear material in use, in storage, and during transport, and for nuclear facilities depending on the associated consequences of either unauthorized removal of nuclear material or sabotage.
- Provide for the regulation of physical protection and include a licensing requirement. The regulations should be applicable to all such materials and facilities regardless of whether under State or private ownership.
- License activities only when they comply with its physical protection regulations.
- Ensure that evaluations also include exercises to test the integrated system, including the training and readiness of guards and/or response forces.
- Determine the trustworthiness policy
- Include enforcement of physical protection regulations as a part of a State's physical protection regime.
- Provide sanctions against the unauthorized removal of nuclear material and against sabotage

Guidance for Other Radioactive Materials

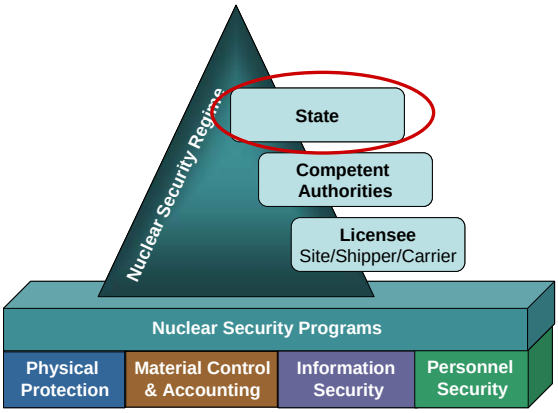
- ***Code of Conduct on the Safety and Security of Radioactive Sources* -** Contains obligations for accountability, physical protection and export/import requirements
- ***Guidance on the Import and Export of Radioactive Sources*** – More detailed guidance on import and export controls

Other Governing Documents

- ***Convention on the Suppression of Acts of Nuclear Terrorism* -** Establishes the acts that will be considered nuclear terrorism and the obligations of States to prevent those acts
- ***Safeguards Agreements and the Additional Protocol* –** Declaration of nuclear materials, safeguards implemented, and facilities for IAEA inspection
- ***UN Security Council Resolution 1373* -** Contains obligations for States to refrain from any form of support to terrorist activities and to prevention of terrorist acts
- ***UN Security Council Resolution 1540* -** Contains obligations for States to develop and maintain appropriate PP measures to prevent the proliferation of nuclear weapons, including the establishment of appropriate control over nuclear material.

Nuclear Security Series

- Technical and Functional Specifications for Border Monitoring Equipment
- Nuclear Forensics Support
- Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators
- Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage
- Identification of Radioactive Sources and Devices
- Combating Illicit Trafficking in Nuclear and other Radioactive Material
- Nuclear Security Culture
- Preventive and Protective Measures against Insider Threats
- Security in the Transport of Radioactive Material
- Development, Use and Maintenance of the Design Basis Threat
- Security of Radioactive Sources
- Educational Programme in Nuclear Security



Nuclear Security Regime - State Responsibilities Relating to Physical Protection

- Establish legal basis for regulations
- Designate competent authority(s)
- Establish nuclear material accountability and control
- Conduct and maintain an intelligence-based threat assessment
- License only facilities and carriers/shippers who meet physical protection objectives
- Provide security transport of nuclear and other radioactive materials
- Designate appropriate response forces

Legal Issues

- Security liability (provide reasonable security)
- Failure to protect (negligence liability)
- Overreaction (excessive force, invasion of privacy, guard instructions and training)
- Labor/employment issues (labor unions, work practices)

Decisions to Be Made

- ☐ Full participation in international agreements
- ☐ Government agency(s) will be responsible for the physical protection of nuclear and radioactive materials
- ☐ Nuclear and radioactive materials permitted in your country
- ☐ Who will conduct an intelligence-based threat assessment and how will decisions be made based on this threat assessment
- ☐ Licensing process and evaluation of continued compliance
- ☐ Level of personnel trustworthiness requirements
- ☐ Classification and associated protection of information and nuclear/radioactive materials
- ☐ Mechanisms for security transport of nuclear and other radioactive materials
- ☐ Response force responsibility
- ☐ Agency for working with legislative body

Summary

- The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State
- The legal framework provides the authorities and penalties associated with nuclear and other radioactive materials
- There are many decisions associated with establishing a nuclear security regime and physical protection program

Module 4
Regulatory Framework

Module Objectives
After completing this module, you should be able to do the following:

- Recognize the legislative and regulatory framework for a physical protection program
- Identify the steps for developing a regulatory approach for a physical protection program
- Identify other regulatory principles

Security and Physical Protection Milestones from Evaluation of the Status of National Nuclear Infrastructure Development (NG-T-3.2)
Milestone 1 – Ready to make a knowledgeable commitment to a nuclear program
Milestone 2 – Ready to invite bids for the first nuclear power plant
Milestone 3 – Ready to commission and operate the first nuclear power plant

Security Conditions and Basis for Evaluation of Milestone 1
15.1 Requirements for security and physical protection acknowledged

- Establishment of a committee for nuclear security related policy making, interagency coordination and planning activities associated with security and physical protection. Clear definition of its role structure, responsibilities, and reporting requirements.
- Evidence of suitable qualifications and experience of the members
- A plan to implement a division/office responsible for the management of security and physical protection arrangements, including an organizational chart, and a description of its function.
- A plan to hire or contract with suitably qualified and experienced experts and organization to assist in security and vulnerability analysis as well as risk assessments of malicious acts to nuclear poser plants, nuclear and other radioactive material and its transportation.
- Government awareness of the risk of malicious acts and possible radiological, political, economical, and social consequences. Evidence of intelligence service technical reports on the analysis of incidents occurring at nuclear facilities in the world.
- Government awareness of international guidelines on security
- Plan to train relevant staff including police and armed forces
- Program to develop strong security culture during Phase 2.

15.2 Necessary regulation identified

- Plan to develop national legislation providing a basis for regulation of security and physical protection arrangements regarding nuclear facilities, nuclear and other radioactive material, its transportation and storage, including provisions for licensing, inspection, and sanctions.
- Plan to develop a regulatory function in the area of security and physical protection, including physical protection requirements, information confidentiality, security staff recruitment, security culture and other components.
- A set of requirements such as those in IAEA Nuclear Security Series.
- A plan, including allocation of adequate resources, for the production of regulatory documents.
- Clear identification of a head organization that will manage a national DBT (design basis threat) development.
- A plan to collect documents, information, data from investigations and other source data on illegal, malicious, criminal and other acts, in order to carry out a risk assessment and modeling scenarios of illegal activities.
- Evidence that external and other threats have been considered for the selected nuclear power plant sites in order to minimize the risk of malicious acts.

15.3 Effective security protection for existing uses of radiation sources in place

- Report of an audit/review of the existing protection against international requirements with a resulting action plan which is being met.

Security Conditions and Basis for Evaluation of Milestone 2

15.1. Legislation promulgated - Arrangements and draft of agreements covering protocols and programs for local and national law enforcement assistance

15.2. DBT defined - The design basis threat defined and outline of security requirements included in the bid invitation specification

15.3. Security requirements defined

- Security requirements and desirable features planned for the site
- Evidence that best practice for security at the nuclear power plant is understood

15.4. Sensitive information defined

- Procedures for the definition and protection of sensitive information
- Penalties for violation available and supported by legislation

15.5. Physical protection by trained on-site security staff provided - Security requirements during construction defined, including on-site civil security personnel and a policy on whether armed, and a plan for their implementation

15.6. Program for selection/qualifications of staff with access to facilities are in place - Adequate screening programs for recruitment and selection of personnel with access to facilities and classified documentation

15.7. Security culture promulgated - Evidence of the promulgation of a security culture, recognizing the importance of nuclear material within all key organizations involved in the nuclear power program

Four Physical Protection Objectives from INFCIRC/225/Rev 5

- Protect against unauthorized removal of nuclear material in use and storage, and during transport;
- Ensure the implementation of rapid and comprehensive measures by the State to locate and recover missing or stolen nuclear material;
- Protect against sabotage of nuclear facilities and sabotage of nuclear material in use and storage and during transport; and
- Mitigate or minimize the radiological consequences of sabotage.

Competent Authority(s) - State agency(s) responsible under national law that have the legally delegated or invested authority, capacity, or power to license and regulate:

- nuclear materials and facilities
- other radioactive materials and facilities that use them
- shippers, carriers, and receivers of nuclear and other radioactive materials

Regulations

- Provide architecture for more detailed conditions and requirements
- Mandatory
- Based on internationally recognized standards and guidelines
- Serve as a basis for licensing and inspections

Guides

- Guidance on how to comply with regulations
- Non-mandatory

Physical Protection Documents

GOV/2001/41 The Physical Protection Objectives and Fundamental Principles was issued by the IAEA Board of Governors in August 2001. It specifies the objectives of physical protection as:

- protect against unauthorized removal of nuclear material in use, storage, or transport,
- ensure rapid measures by the State to locate and recover missing or stolen nuclear material,
- protect against sabotage of nuclear material and facilities
- mitigate or minimize the radiological consequences of sabotage.

It also provides 12 Fundamental Principles that serve as a basis for achieving the physical protection objectives. The PP objectives and Fundamental Principles from GOV/2001/41 were adopted into the amendment to CPPNM.

INFCIRC/225 The Physical Protection of Nuclear Material and Nuclear Facilities provides recommendations for protection of nuclear materials in use, storage, and transport against theft and sabotage.

- Provides a set of recommendations on requirements for the physical protection of nuclear material in use and storage and during transport and of nuclear facilities
- Provides a categorization of the different types of nuclear material
- Links protection levels to categories of material
- Currently under revision to address the current threat environment and ensure conformance to CPPNM

Guidance and considerations for the implementation of INFCIRC/225/Rev4, Technical Document (TECDOC 967) provides additional guidance on how to implement INFCIRC/225 recommendations.

Handbook on the physical protection of nuclear materials and facilities (TECDOC 1276) is a handbook for use in design, operation, and maintenance of physical protection systems.

Nuclear Security Series Framework
http://www-ns.iaea.org/security/nuclear_security_series.htm

Nuclear Security Fundamentals - contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations

- Nuclear Security Fundamentals (Objectives and Essential Elements) [in final stages]

Recommendations - present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals

- Recommendations for the Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev 5)
- Recommendations for the Security of Radioactive Materials and Associated Facilities
- Recommendations for Detection and Response

Implementing Guides - provide further elaboration of the recommendations in broad areas and suggest measures for their implementation

- Nuclear Security Culture (NSS-7)
- Confidentiality of Nuclear Security Sensitive Information
- Preventative and protective Measures Against Insider Threats (NSS-8)
- Security in the Transport of Radioactive Materials (NSS-9)
- Security of Radioactive Sources (NSS-11)
- Design Basis Threat (NSS-10)
- Protection Against Sabotage
- Radioactive Waste Security
- Physical Protection of Nuclear Materials During Transport
- Nuclear Security at Major Public Events

Technical Guidance

- **Reference Manuals**, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities;
- **Training Guides**, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and
- **Service Guides**, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions

Technical Guidance

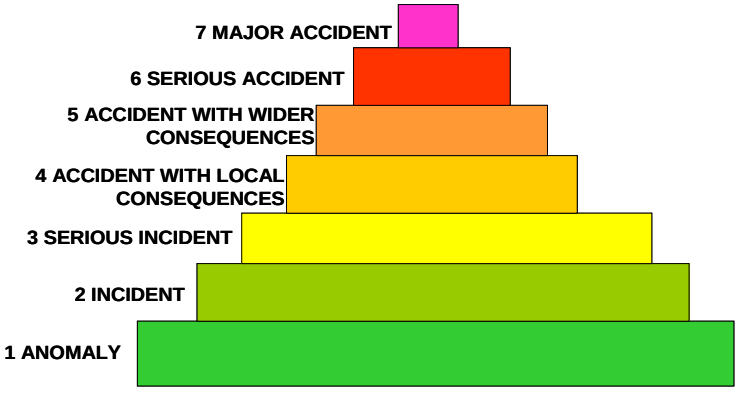
- Nuclear Security Glossary
- Model Regulations for Security Nuclear and Other Radioactive Material and Associated Nuclear Facilities
- Education Program for Nuclear Security (NSS-12)
- Engineering Safety Aspects for the Protection of Nuclear Power Plants Against Sabotage (NSS-4)
- Identification of Vital Areas of Nuclear Facilities
- INPRO Manual on Physical Protection
- Physical protection of Research Reactors and Associated Facilities
- Security of Information and Instrumentation of Control Systems at Nuclear Facilities
- Security of Fissile Material in Transport
- Nuclear Material Accounting Systems at Facilities
- Nuclear Forensics Support (NSS-2)
- Technical and Functional Specifications for Border Monitoring Equipment (NSS-1)
- Monitoring for Radioactive Materials in International Mail (NSS-3)
- Identification of Radioactive Sources and Devices (NSS-5)
- Combating Illicit Trafficking in Nuclear and Other Radioactive Material (NSS-6)
- Procedures for Examining Legal Shipment of Radoactive Material for the Detection of Illegal Activities
- Detection and Response for Radioactive Material at Seaports

Basic Steps for Developing a Regulatory Framework

- Define undesired consequences
- Establish graded Security Levels with corresponding protection goals
- Correlate nuclear and other radioactive materials to Security Levels
- Select and implement a regulatory approach

Undesired Consequences

- Loss of Life/Severe Injury
- Economic Loss
- Environmental Contamination
- Political Upheaval/Loss of Public Confidence



Nuclear and Radiological Event Scale

Graded Protection Approaches - The application of physical protection measures proportional to the potential consequences of a malicious act.

- Target categorization tables provide a means to apply graded levels of protection.
- Different graded approaches may be considered:
  - Grade system effectiveness – all systems use the same Design Basis Threat (DBT) but require less effective systems for lower consequence targets
  - Grade the threat for targets – all targets/systems meet the same level of performance, but the lower-consequence targets use a lower-level threat
  - Grade both system effectiveness and threat for targets

IAEA Categorization of Nuclear Material from INFCIRC/225

Material	Form	Category I	Category II	Category III[c]
1. Plutonium[a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235	Unirradiated[b] – uranium enriched to 20% ^{235}U or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15 g
	– uranium enriched to 10% ^{235}U but less than 20% ^{235}U		10 kg or more	Less than 10 kg but more than 1 kg
	– uranium enriched above natural, but less than 10% ^{235}U			10 kg or more
3. Uranium-233	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated Fuel (The categorization of irradiated fuel in the table is based on international *transport* considerations. The State may assign a different category for domestic use, storage, and *transport* taking all relevant factors into account.)			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[d/e]	

a) All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
b) Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/hr
c) Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.
d) Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.
e) Other fuel which by virtue of its original material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/hr (100rad/hr) at one meter unshielded.

Example of Security Levels Based on Nuclear Materials

- Category I – Strategic Special Nuclear Material
- Category II – Special Nuclear Material of moderate strategic significance
- Category III – Special Nuclear Material of low strategic significance

Goal: To establish conditions that minimize the possibility of *sabotage* and/or *unauthorized removal* of nuclear material

Radioactive Sources
Radioactive source means a radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. (Code of Conduct on the Safety and Security of Radioactive Sources (INFCIRC/663)).

The A/D ratio is the ratio of the total source activity based on quantity in use versus the deterministic source activity for “damage” to humans. Category I source material has the highest risk of the sources. There are five categories. (Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency; Updating IAEA-TECDOC-953 and Categorization of Radioactive Sources; IAEA-TECDOC-1344).

Categorization Table for Radioactive Materials from NNS-11

Category	Source	A/D	Security level
1	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	A/D ≥ 1000	A
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D ≥ 10	B
3	Fixed industrial gauges that incorporate high activity sources Well logging gauges	10 > A/D ≥ 1	C
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D ≥ 0.01	Apply measures as described in the Basic Safety Standards [5]
5	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt	

Example of Security Levels for Radioactive Sources
The IAEA recommends the following Security Levels and associated goals for radioactive materials in the Security of Radioactive Sources; IAEA-TECDOC-1355:

> **Security Level A:** Measures should be established to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner. These measures should be such as to delay acquisition until response is possible to prevent unauthorized removal of a source (timely detection and response).
>
> **Security Level B:** Measures should be established to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner to minimize the likelihood of unauthorized removal of a source (immediate detection of the unauthorized removal, but not requiring a response to interrupt the act)

Security Level C: Measures should be established to deter unauthorized access and verify the presence of the source at set intervals to reduce the likelihood of unauthorized removal of a source reduce the likelihood of unauthorized removal of a source

Threat - Design Basis Threat (DBT)

- State regulatory tool used for planning, designing, and evaluating a PPS
- Covers both theft and sabotage
- Describes attributes and characteristics of potential adversaries
- Not an explicit description of the expected adversary:
    - Provides basis for State-wide consistency
    - May change as events occur
    - Supports prudent PPS within cost constraints

Regulatory Approaches

- Prescriptive (three-meter-high fence, sensors in storage area)
    - Advantage – Easy to apply
    - Disadvantage – No assurance of desired performance
- Performance-based (Have performance effectiveness greater than *yy*)
    - Advantage – Identifies effectiveness
    - Disadvantage – more difficult to apply, requires expertise
- Combination of the two
    - Uses both feature and performance requirements
        - Feature requirements where quantification is difficult
        - Performance requirements should be in as many areas as feasible
    - The combination leads to improved cost-effectiveness

Approach Comparison

Approach	System Goal	Effectiveness Measures
Prescriptive Criteria	Include required features (Example: three perimeter sensors required)	Number of features present or feature performance
Performance Criteria	Meet PPS objectives (Example: perimeter system to detect intruder)	Overall system performance
Combined Prescriptive and Performance	Apply feature or performance criteria as appropriate to meet PPS objectives	Overall performance or feature presence

Nuclear Security Regulatory Architecture

1. **Licensing**
2. **Definitions**
    a) Information and Material Classification System
    b) Design Basis Threat
3. **Requirements for each type of material**
    a) Personnel Trustworthiness
    b) Physical Protection Systems
    c) Response Force
    d) Information Security
    e) Material Control and Accounting
    f) Import/Export
4. **Considerations**
    a) Security Culture
    b) Defense-in-Depth
    c) Confidentiality
    d) Contingency Planning
    e) Emergency Preparedness/Response
    f) Quality Assurance

Consideration: Nuclear Security Culture (NSS-7)

The assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security

- Nuclear Security Culture: all organizations involved in implementing physical protection should:
    - Give due priority to the security culture
    - Provide for its development and maintenance
    - Ensure its effective implementation in the entire regime
- Radioactive Sources Security Culture
    - Every State should, in order to protect individuals, society, and the environment, take the appropriate measures to ensure … the promotion of safety culture and of security culture with respect to radioactive sources.

Consideration: Defense-in-Depth

The State's requirements for physical protection should reflect a concept of several layers and methods of protection that have to be overcome or circumvented by an adversary in order to achieve adversary objectives:

- Structural
- Technical
- Personnel
- Organizational

Consideration: Confidentiality

- Requirements for protecting the confidentiality of information
- Applicable when unauthorized disclosure could compromise the physical protection of nuclear material and nuclear facilities

Consideration: Contingency Planning to respond to**:**

- Unauthorized removal of nuclear material
- Sabotage of nuclear facilities or nuclear material
- Attempts at either

Consideration: Emergency Preparedness/Response – compensatory measures to respond to:

- Failure of physical protection equipment
- Reduced security personnel status
- Medical emergencies

Consideration: Quality Assurance

Policy and program established to provide confidence that specified requirements for all activities important to physical protection are satisfied:

- Inspections
- Performance Testing
- Change Management

Decisions to be Made

- ☐ Develop a regulatory approach
- ☐ Establish regulatory framework covering:
    - Licensing
    - Definitions
    - Requirements
    - Considerations
- ☐ Graded approach framework

Summary

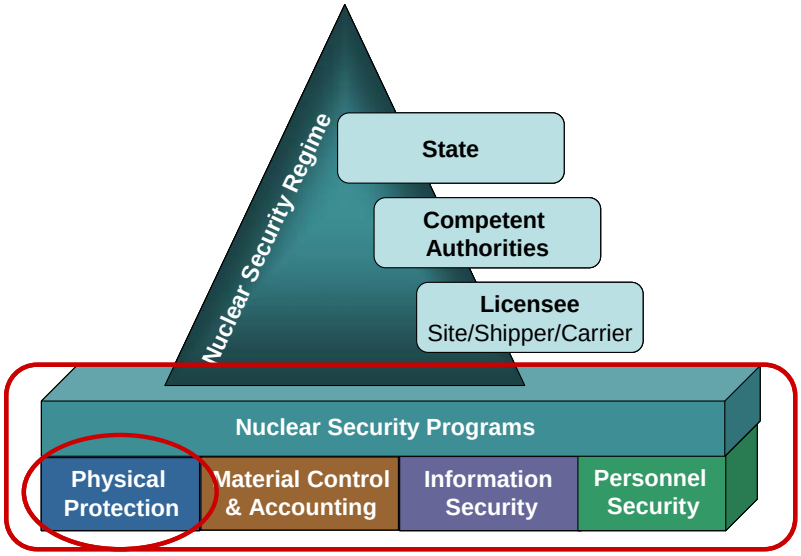
- Legal and regulatory framework comes from the IAEA and international community
- The IAEA provides guidance to categorize nuclear and radiological material consequences
- Both feature-based and performance-based regulatory approaches may be used to specify PPP requirements
- Developing and maintaining a nuclear security culture is an important regulatory principle.

Module 5
Overview of Nuclear Security Programs and Their Relationship to Physical Protection

Module Objectives
After completing this module you should be able to do the following:

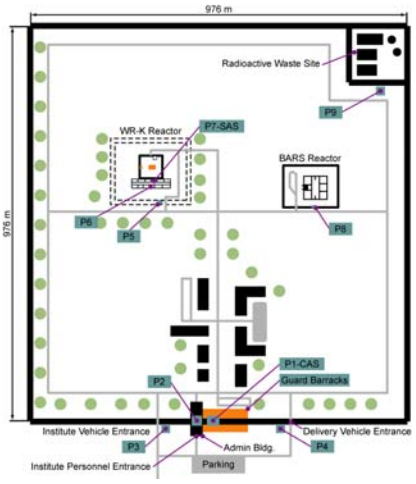
- Describe the four programs that support a Nuclear Security Program
- Describe a Physical Protection Program
- Describe the relationship between Material Control and Accounting, Information Security, Personnel Security and Physical Protection
- Describe the decisions that must be made to support Physical Protection

Nuclear Security Reference Model



Physical Protection Program

A physical protection program, is the integration of people, procedures, and equipment used to protect assets or facilities against theft, sabotage, or other malicious human attacks.



Fixed Site Physical Protection System

Fixed site application usually provides physical protection for nuclear or other radioactive materials contained in buildings or facilities on a site. Depending on the nature of the materials, the site may or may not include multiple layers of protection.

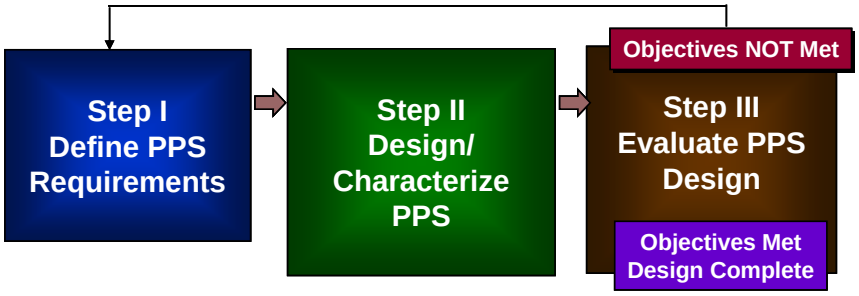
Transportation Physical Protection System

- Material movement within a site
- Material movement to and from a site

Design and Evaluation Approaches

Approach	Requirement	Metric
Expert	Satisfy expert	Opinion
Prescriptive	Include required features	Presence of features
Component Criteria	Include required features that meet specific standards	Presence of feature and performance standard
Performance	Prevent theft or sabotage of nuclear material	System effectiveness

A System Engineering Process – Three Interdependent Steps



Repeat process until risk is acceptable

Define Requirements

- Understand the threat
- Identify the assets of interest
- Characterize the environment
- Existing facility or facility design
    - Operational states
    - Employee populations
    - Existing physical protection
    - Terrain, climate, weather, etc.

Physical Protection Goals

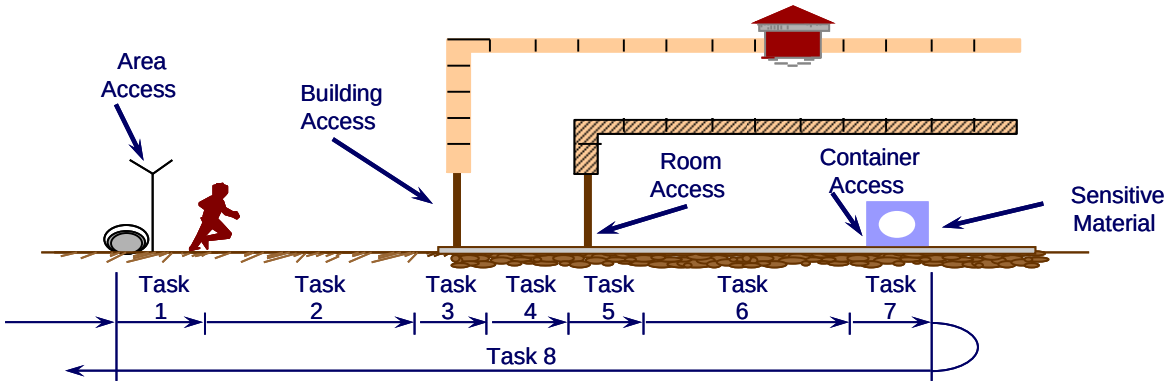
- Deter attack
- Detect attack as it begins and as it progresses
- Increase adversary time to complete task through delay
- Respond to attack in timely and effective manner

PPS Functions – Can use technology or guards to perform

- Detection
- Delay
- Response

Security Event Sequence Example

For a successful system design, the total time for detection, delay, and response must be less than adversary task time to complete his or her goal



Security Risk

- Exposure to the possibility of future harm or loss due to malicious actions of persons or groups of persons
- A function of
    - Frequency of loss describing how often do malicious actions take place
    - The consequence–a measure of harm or loss–that will occur if a malicious action takes place
    - The effectiveness of protection and mitigation measures
- The amount of control each licensee has over each function is different

Risk Management

- **Risk avoidance** is accomplished by eliminating the source of the risk. For example moving nuclear or radioactive materials out of a building that cannot adequately protect it to a building specifically designed to protect those kinds of materials.

- **Risk reduction** is achieved by taking some actions to lower risk to the community/facility to reduce the severity of the loss. This is the objective of many security programs – to lower risk by implementing at least some security measures.
- **Spreading the risk** can be accomplished by having similar services/ processes/assets at more than one facility site. By separating assets, fewer assets are at risk during any given adversary attack.
- **Risk transfer** is the use of insurance to cover the replacement or other costs incurred as a result of the loss.
- **Risk acceptance** is the recognition that there will always be some residual risk.

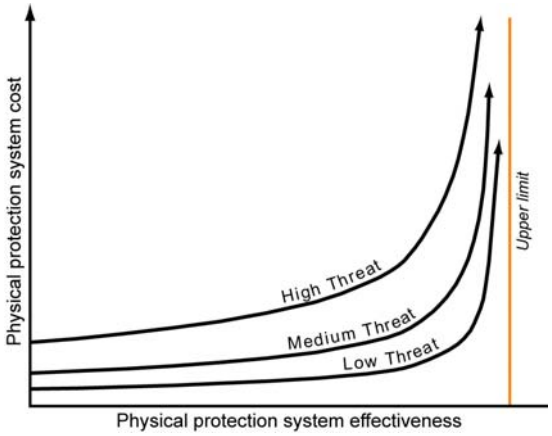
Risk Reduction Strategies

There are a number of strategies for risk reduction in a State's nuclear program:

- Consolidation to fewer locations
- Conversion to less attractive materials
- Final disposition of excess materials
- Cost-effective physical protection systems

Cost vs. System Effectiveness

The Competent Authority will have to determine how much risk is acceptable vs. the cost of reducing that risk.



Physical Protection System Summary

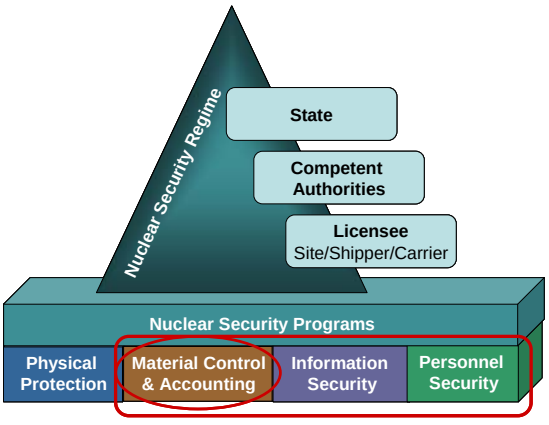
A physical protection system is the integration of **people, procedures, and equipment** used to **protect assets or facilities** against **theft, sabotage**, or other malicious human attacks.

- Fixed sites
- Transportation
- Risk component

Material Control and Accounting (MC&A)

The MC&A Program functions as a whole to

- Provide information on the location and use of strategic nuclear materials
- Provide assurance that they are accessed and processed in a manner appropriate to their strategic significance
- Monitor that the facilities, personnel, and regulations are adequate to deter and



Nuclear Security Reference Model

detect diversion of nuclear material from its intended purposes
- Be able to state that ‘the nuclear material was adequately accounted for’

Why is MC&A Important?

- To provide assurance that nuclear materials are accounted for properly.
- To detect theft or diversion of nuclear materials.
- To act as an integral component of the safeguards system that deters theft or diversion of nuclear materials.
- Or, how do we really know when and how much nuclear material is missing, and how do we deter the potential diverter?

Accountable Nuclear Materials

Those defined in the guidance documents:

- Fissile Materials (Enriched Uranium, Plutonium, Neptunium, Americium)
- Source materials used to produce fissile materials (Depleted and Normal Uranium, Thorium)
- Other materials of special interest, e.g. Tritium, Californium, Curium

Other Radioactive Materials of Concern

Code of Conduct on the Safety and Security of Radioactive Sources

- **Am-241**
- **Am-241/Be**
- **Cf-252**
- **Cm-244**
- **Co-60**
- **Cs-137**
- **Cd-153**
- **Ir-192**
- **Pm-147**
- **Pu-238**
- **Pu-239/Be**
- **Ra-226**
- **Se-75**
- **Sr-90(Y-90)**
- **Tm-170**
- **Yb-169**

Main Components of MC&A Program

- ***Accounting***
  - Provide a complete, accurate, and timely record of the nuclear material inventory
  - Determine the nuclear material inventory
  - Document nuclear material transactions/movements
  - Issue periodic reports
  - Assist with the detection of material gains or losses, unauthorized data access, and data falsification
  - Provide a complete audit trail for all nuclear material from receipt through disposition
  - Provide a complete, accurate, and timely record of the nuclear material inventory

- ***Measurements and Measurement Control***
  - Measurements are used to establish and/or confirm the amount of nuclear material present in a specific item, container, or in some cases facility. These measurements may be destructive or nondestructive, but conducted within a measurement control system.
  - The Measurement Control system is designed to ensure measurement stability, establish measurement uncertainty, and to ensure measurements meet the quality objectives required by the safeguards system.
  - All of these efforts are ultimately designed to provide confidence in measurement results and assurance that the measurement uncertainties are well known and adequate for their needs

Main Components of MC&A Program (continued)

- ***Material Control***
    - Controls the location and use of nuclear materials through appropriate systems of containment and surveillance
    - Ensures that nuclear materials are used, processed, or stored only in areas that have been identified for these purposes.
    - Provides sealing and containment for materials that are being stored or transported.
    - Establishes boundaries where nuclear materials can be located, along with controls for these boundaries, and provides controls governing the use of materials within these boundaries.
    - Accomplished with people, procedures and technology and includes
        - Access requirements for facilities, nuclear information databases, areas within a facility, etc.
        - Covering procedures for handling, processing, inventorying and reporting on nuclear materials
        - Personnel surveillance when working in nuclear material areas
        - Material containment and surveillance systems

- ***Assessments***
    - Ensure the integrated MC&A system is capable of detecting and assessing unauthorized removals of nuclear material
    - Ensure that detection elements provide sufficient information to correctly assess alarms and to quantify and localize losses
    - Monitor and evaluate:
    - Inventory differences
    - Shipper/Receiver differences
    - Anomalies
    - Related statistical/confidence limits
    - Routinely evaluate the MC&A system by introducing anomalies to determine if these artificial anomalies are detected
    - Assess unauthorized removals of nuclear material

Unsuccessful MC&A - What can happen when MC&A isn't effective?

- Shutdown of operations
- Undiscovered Diversion/Theft
- Unexplained Loss
- Poor Criticality Safety
- Poor Environmental Stewardship
- Loss of Credibility with citizens, international community, United Nations
- Successful adversarial attacks

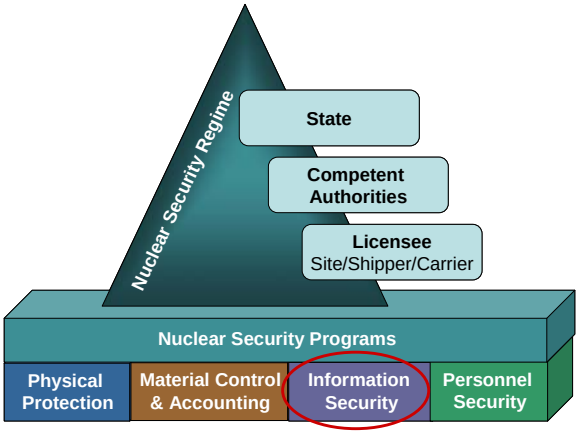
Impacts to Physical Protection

- Material unaccounted for can result in security events to which the physical protection system must respond
- Material categorizations can determine the level of physical protection required
- Access to material must be controlled through the access control system in a physical protection system

Information/Cyber Security

Requirement for Confidentiality

- Requirements for protecting the confidentiality of information (one of the 12 fundamental principles)
- Applicable when unauthorized disclosure could compromise the physical protection of nuclear material and nuclear facilities
- Nuclear Security Reference Model



Nuclear Security Reference Model

Information Systems – systems where information is stored, used, or transmitted

- Physical
  - Paper-based systems
  - Policies, procedures, access control lists
- Cyber
  - Electronic or network based systems

Threats to information systems have significant consequences

- Theft of classified information or materials
- Loss of services – internal and external
- Contamination of surrounding population

Who are the adversaries? Insiders? Outsiders?

Cyber adversaries characterized by

- Commitment
  - Intensity
  - Stealth
  - Time
- Resources
  - Technical Personnel
  - Cyber/Kinetic Knowledge
  - Access

Common Cyber Adversary Tools

- **Virus** – a self-executing/self-replicating program written to alter the way a computer operates without the permission or knowledge of the user
- **Worm** – programs that replicate themselves from system to system without the use of a host file, usually embedded in documents
- **Denial of Service** – attacks that overload the system so that it is not available to authorized users
- **Remote Access Capabilities** – attacks that allow access to a system through backdoors or remote access features

Information Security Protection Measures

Administrative Controls

- Training
- Policies and procedures
- Principle of Least Privilege
- Administrative Controls (similar to access control)

Password Management

- Change often
- Every 6 months or annually
- Whenever possibly compromised
- Limit number of failed password attempts
- Immediately delete user accounts when personnel terminate employment or contracts are terminated

Technical Controls

- Network Design and Configuration Management
- Detection and Logging
- Firewalls
- Routers
- Virus Protection

Mitigation/Recovery

- Policies, architectures, frameworks, and accountabilities used to lessen risk by lower its chances of happening or reducing its effect if it does occur
    - Graceful degradation while under attack
    - Survivable functions
    - Network isolation
    - Recovery of systems/data
    - Compensatory measures
- Periodic backups/mirror images made, tested, and protected at the same level as the original, but not at the same location

Physical Protection & Information Systems

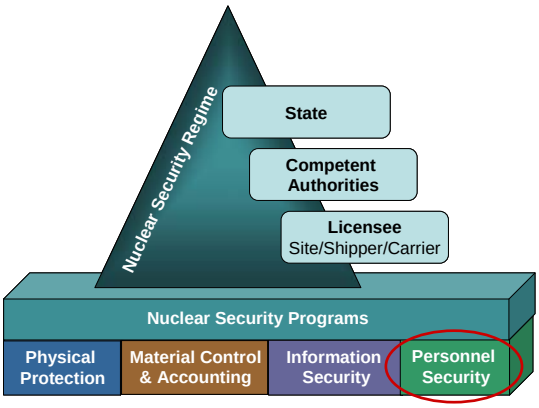
- Physical Protection of Information Systems
  - Critical assets that must be protected
- Cyber Systems are part of Physical Protection Systems
  - Access controls
  - Sensor and alarm communications

Information Security Summary

- The consequences of loss of information systems, whether paper or cyber, can be costly
- Ensure access control, cyber systems, and physical protection systems are integrated under a common security umbrella
- Ensure physical protection information systems are kept isolated from other information systems

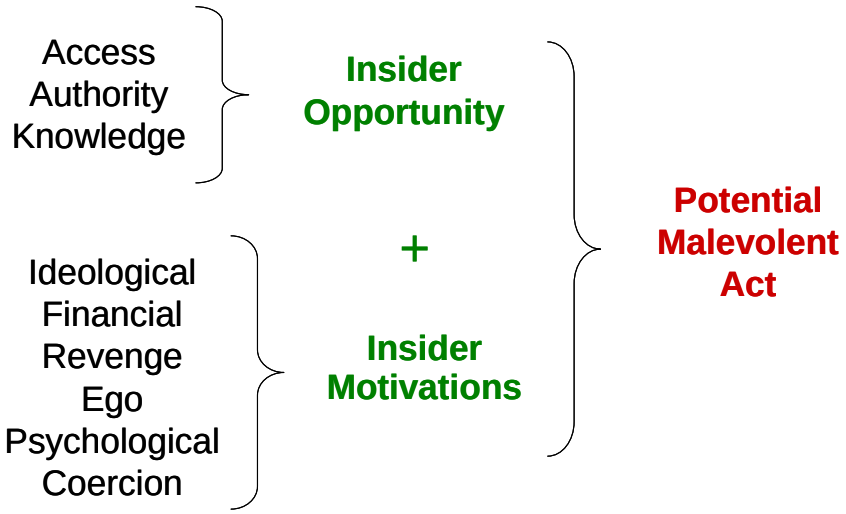
Personnel Security

Discussion
Who is the greater threat - the insider or the outsider? Why?

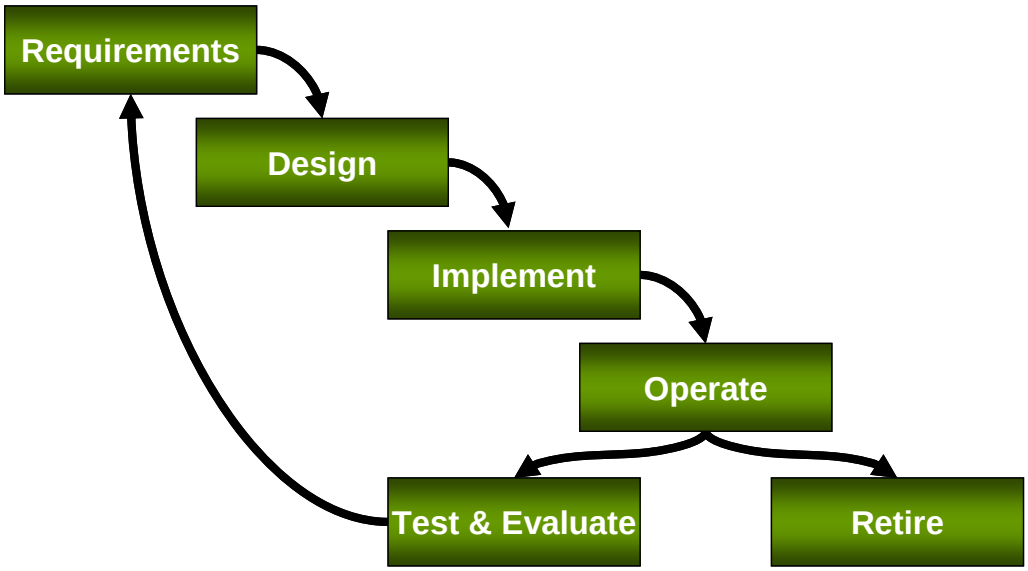


Nuclear Security Reference Model

Potential for Malevolent Act



Facility Life Cycle – Vulnerabilities can be introduced by people at any stage of the system



People – The Human Factor

- Most security assumes that people follow the rules.
- People tend to take the path of least resistance.
- People can be your best detectors or your worst adversaries.
- Contributor to all nuclear security incidents
    - Personnel errors
    - Ergonomic issues
    - Inadequate organizational procedures and processes
    - Management failures

Nuclear Security Culture

Ensure all personnel are knowledgeable of and proficient in MC&A requirements:

- Document all requirements in accordance with graded risk dependent upon attractiveness of the nuclear material.
- Proceduralize personnel activities when processing nuclear material to incorporate these requirements.
- Qualification of personnel through a system based on knowledge, experience, and training.

Personnel Security Program

- Nuclear Security Culture - Shape attitudes and beliefs
- Personnel trustworthiness program - Seeks to address motivations
- Graded access control/privileges
    - Least privilege
    - Mitigates access and other insider advantages
- Data monitoring and logging - Reduces insider opportunities for malicious activity without exposure

Personnel Security Summary

- Elements of a Personnel Security Program
    - Nuclear Security Culture
    - Personnel trustworthiness program
    - Graded access control/privileges
    - Data monitoring and logging
- People are the key to Nuclear Security

Decisions to be Made

- Physical protection system
    - Need classification system for protection of information and materials
    - State adopted material categorization definition
    - Define design and evaluation process
- Material control and accounting
    - What material will be accepted in the state
    - Associated material levels of protection
    - Material accounting system
    - Material control system
- Information Security
    - Classification system for information and materials
    - Process of certification and accreditation of information system
    - Process for evaluation of information systems
    - Separation of information systems
- Personnel Security
    - Personnel trustworthiness program
    - Personnel identification system
    - Access and privileges levels

Summary

- The Physical Protection Program is an element of a Nuclear Security Program.
- MC&A, Information Security, and Personnel Security all impact the physical protection program in some fashion.

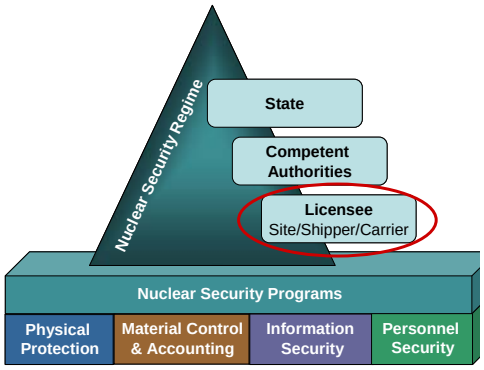
Module 6
Requirements Definition

Module Objectives
After completing this module you should be able to do the following:

- Identify the three questions used to define PPS requirements
- Identify the targets of concern in PPS design
- Define design basis threat (DBT)
- Explain how performance requirements are specified

Physical Protections Systems
The licensee has the responsibility for designing and implementing effective physical protection systems

Physical Protection System
A physical protection system is the integration of people, procedures, and equipment used to protect assets or facilities against theft, sabotage, or other malicious human attacks.



Nuclear Security Reference Model

A System Engineering Process
The Design and Evaluation Process contains three major steps:

1. Define physical protection system requirements by characterizing the facility, understanding the assets, and defining the adversary
2. Design/characterize a physical protection system in terms of detection, delay, and response functions.
3. Evaluate the physical protection system design or implementation for system effectiveness

Lastly, a decision is made to determine if the design/implementation is acceptable and if not, then a re-evaluation of the assumptions is made (e.g., the consequence assessment) and/or a redesign/upgrade is required

Three Essential Questions that define the requirements for a PPS

1. What assets must be protected to prevent undesired consequences?
2. What threat must be protected against?
3. What level of protection is adequate?

1. What must be protected?

- Nuclear materials
- Nuclear facilities
- Radioactive sources in the facilities
- Information
- People
- Environment

Some Undesired Consequences of Malicious Acts

- Damage to national security
- Successful terrorist attack
- Loss of control of nuclear material or weapons
- Loss of life as a result of hazardous material release
- Theft of material or information
- Interruption of critical utilities such as water, power, or communications
- Degraded business operations
- Loss of market position
- Workplace violence, extortion, blackmail
- Damage to reputation
- Legal liability

Examples of Metric of Undesired Consequences

- **Injury**
  - Number of injuries
  - Severity of injuries
- **Environment**
  - Total hectares contaminated
  - Value of hectares
  - Loss of use
- **Political**
  - Stability of government
  - Public trust
- **Economic - Costs of Act**
  - Cleanup and food embargo
  - Loss in productivity
  - Legal costs
  - Value of facilities, etc., damaged
  - Ransom

Targets—What are they?

- Theft Targets
  - Nuclear or radioactive materials
  - Information
  - People
- Sabotage Targets
  - Nuclear or radioactive materials
  - Process or support equipment needed to prevent unacceptable radiological consequences

2. What threats must be protected against?

- The competent authority must define a threat that the physical protection system (PPS) is expected to withstand.
- The defined threat specifies the adversary attributes and characteristics that the PPS must be designed to defend against.
- This is commonly referred to as the design basis threat (DBT).

Definitions

Threat Spectrum - A range of adversary types (may be low to high) against which the site and assets will be analyzed (should include maximum credible adversary). May be outsider or insider.

State Threat Assessment - A judgment, based on analysis of available intelligence, law enforcement, and open-source information, of the actual or potential threat to one or more facilities or programs.

Design Basis Threat- A selected threat defined by attributes and characteristics against which a physical protection system is designed and evaluated. Typically, DBT is only used for high consequence facilities such at Category 1 facilities and nuclear power plants.

High Consequence Facility - Those facilities whose failure or disruption could be potentially associated with the highest possible impact among all the facilities.
Much of this determination will be a function of the risk tolerance of the enterprise that owns the facilities, but some facilities have an unacceptably high consequence of loss and must be protected.

Design Basis Threat

- State regulatory tool used for planning, designing, and evaluating a PPS (Cat I and nuclear power plant)
- Four components:
    - Malicious acts (theft, sabotage) and unacceptable potential consequences
    - Threat spectrum of potential insider/external adversaries
    - Adversary attributes and characteristics
    - Performance basis for design and evaluation
- Not an explicit description of the expected adversary:
    - Provides basis for State-wide consistency
    - May change as events occur
    - Supports prudent (less than Cat III) PPS within cost constraints

The Value of a Design Basis Threat (DBT)

The DBT provides a rational basis for the following:

- Making and justifying decisions
    - By the operators
    - By the competent authority
- The design of a physical protection system
    - Ensuring sufficient countermeasures
    - Avoiding unnecessary countermeasures
- Evaluating the adequacy of a physical protection system

Categories of Adversary

- Outsider Threat - Any individual (or group of individuals) without authorized access to nuclear facilities or transport who might attempt unauthorized removal or sabotage, or who might assist insiders in these activities including
    - Terrorists
    - Criminals
    - Protesters
    - Others

- Insider Threat - Any individual (or group of individuals) with authorized access to nuclear facilities or transport who might attempt unauthorized removal or sabotage, or who could aid outsiders in these activities including:
    - Management
    - Regular employees
    - Security personnel
    - Service providers
    - Visitors
    - Inspectors
    - Former employees

- Collusion Threat – Insiders and outsiders working together to achieve adversary goals

Example DBT Outsider

- Four well-trained terrorists with military weapons and explosives, plus all commercially available hand and power tools
- Two criminals with handguns and small hand and power tools
- Six protesters with hand and power tools
- Intention: unauthorized removal of radiological materials
- Add tools inside facility
- Collusion: possible with an employee

Example DBT Insider

- Number: one in any position
- Type: up to and including active-violent
- Intentions: Steal material or commit radiological sabotage against facility and personnel
- Collusion: acts alone while on-site
- Equipment:
    - Tools existing in facility
    - Contraband brought into facility, including small arms or explosives

Identify What Needs to be Known About the Threat

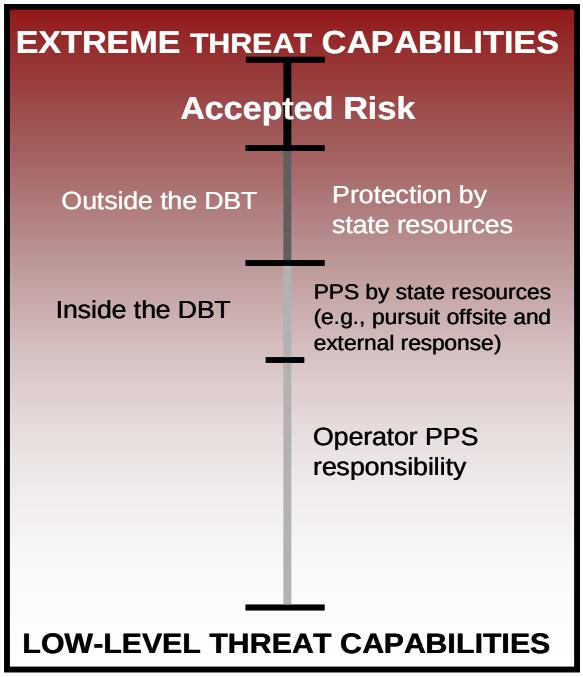
- Motivation - Ideological, Personal, Economic, Psychotic, or Other
- Intention - Theft or Sabotage
- Capabilities
  - ☐ Group Size
  - ☐ Weapons
  - ☐ Explosives
  - ☐ Tools
  - ☐ Transportation
  - ☐ Skills
  - ☐ Funding
  - ☐ Collusion with Insider
  - ☐ Support Structure

Maintaining a DBT

- Formal review process should be used to ensure validity of DBT
- Triggers for DBT review include
  - Event that indicates unexpected threat
  - Change in government policy
  - Change in nuclear program or nuclear material
  - Request by interested party
  - Periodic review
- Same process is used as for developing a DBT
- Review may or may not result in change to DBT

3. What level of physical protection is adequate?

- Objective: reduce the risk associated with use of nuclear or other radioactive materials to an acceptable level
- Must strike a balance between risk, beneficial use, and costs
- The level of security should reflect the potential consequences of misuse of the source: higher potential consequences imply higher levels of security (i.e. graded approach)



DBT Space

DBT Space

- Threat spectrum extends from low threat (capabilities) to high threat: threat assessment addresses full spectrum
- DBT is regulatory tool for physical protection in a performance-based approach to requirements, design, and evaluation
- State requires protection against some threats with capabilities greater than the DBT
- Licensees have primary responsibility for protection against the DBT

Decisions to be made

- What needs to be protected?
- What threats to protect against?
- What level of protection is adequate?

Summary

- PPS Requirements Definition
    - Targets - What assets must be protected to prevent undesired consequences?
    - Threats - What threat must be protected against?
    - Performance Metric - What level of protection is adequate?
- Targets of concern include nuclear materials and facilities and radioactive materials.
- The DBT is the set of threat characteristics a physical protection system is designed to counter in order to prevent undesired consequences.
- Performance requirements may be feature-based (prescriptive), performance-based, or a combination of both of these approaches.

Module 7
Facility Characterization and Siting Impacts

Module Objectives

- After completing this module you should be able to do the following:
- Recognize the role of facility siting
- Recognize the role of characterizing a site and physical protection design
- Identify elements of site characterization
- Identify elements of physical protection design characterization

Characterization Considerations

- If building a new site, choose the site carefully with physical protection in mind.
- Design the PPS into the site design.
- This approach is much cheaper than adding the PPS after the site and its facilities have been built.

Siting Considerations

- Location Considerations
    - Population centers
    - Nearby businesses/structures
    - Nearest emergency response group
    - Security response force location
    - Availability and reliability of power and communications
    - Proximity to labor pool
    - Local crime
    - Wide-open spaces
- Environmental Considerations
    - Topography at the site
    - Vegetations and wildlife
    - Background noise
    - Climate and weather
    - Soil conditions
    - Water flows/drainage

Other Considerations

- Safety/Security Interactions
    - Safety is concerned primarily with the prevention of accidental events (injuries)
    - Security is concerned primarily with the prevention of intentional malicious attacks (theft, sabotage)
- Legal
    - Security liability - Provide reasonable security
    - Failure to protect - Negligence liability
    - Overreaction - Excessive force, lethal force, invasion of privacy, and rules of engagement
    - Labor/employment issues - Labor unions, work practices

- Political
    - Surrounding community relations
    - Facility and local law enforcement liaison
    - Mutual aid agreements - Memorandums of understanding with military organizations, local law enforcement agencies, other facilities, etc.

The Role of Characterization

- Establishes a baseline
- Provides input to system effectiveness evaluations
- Identifies potential weaknesses in physical Protection Systems
- Facilities can be characterized using
    - Concept of operations
    - Existing site information
    - Open sources

Site Characterization

- Vital Areas
- Physical Conditions
- Operational Conditions
- Non-Standard/Emergency Conditions
- Physical Protection System
- Infrastructure
- Siting – see siting considerations above

Vital Area Identification - Areas in high consequence facilities containing

- Nuclear material or other radioactive materials
- Equipment, systems, or devices to be protected against sabotage resulting in
- Exposure of people to radioactivity
- Release of radioactivity to the environment

Physical Conditions

- Site boundaries, fences, barriers,
- Building's construction materials for walls, ceilings, floors, doors, windows, etc.
- Areas and rooms
- Access points
- Environmentally-controlled areas
- Locations of non-target, hazardous material

Operational Conditions

- Operational activities
- Products and processes
- Operational hours/shifts

- Number, types, and locations of employees
- Visitors and vendors
- Access management
- On-site location and movement of materials

Non-Standard/Emergency Conditions

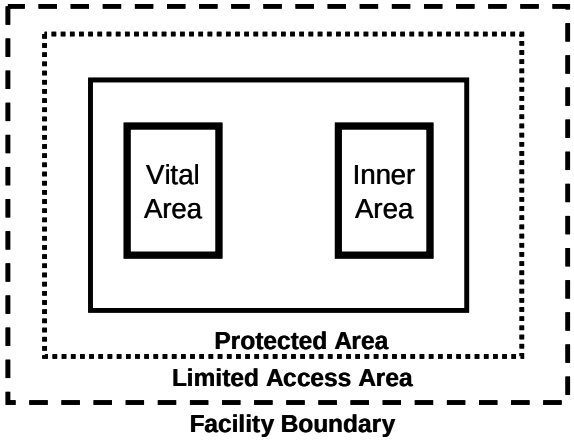
- Equipment failures
- Maintenance
- Medical emergency
- Unusual weather – fog, rain, wind, snow, hurricane, etc.
- Labor dispute
- Fire

Physical Protection System - Characterize existing system or new design in terms of

- Protection Layers
- PPS Functions
- Detection and Assessment
- Delay Mechanisms
- Response
- Policies and Procedures

Identify Protection Layers and Associated Security Areas

- Limited access area – Designated area containing a nuclear facility and nuclear material to which access is limited and controlled for physical protection purposes.
- Protected area – Area inside a limited access area containing Category I or II nuclear material and/or sabotage targets surrounded by a physical barrier with additional physical protection measures.
- Inner area – An area with additional protection measures inside a protected area, where Category I nuclear material is used and/or stored.
- Vital area – An area inside a protected area containing equipment, systems or devices, or nuclear material the sabotage of which could directly or indirectly lead to high radiological consequences.



Facility Policies and Procedures

- Written and unwritten policies/procedures - Frequently, procedures in use are not implemented as described in the documentation. Examples:
    - Policies for handling email, OUO material, proprietary information, site information
    - Procedures for responding to alarms, unauthorized personnel, what cannot be brought into controlled areas
- Training security policies and procedures
    - Frequency of training
    - How it is delivered
    - What it must cover
    - How changes are promulgated
- Other indications of nuclear security culture
    - Values practiced at the site
    - Management adherence or exceptions to procedures and policies

Infrastructure - Availability and reliability of the following:

- Heating, ventilation, air conditioning
- Communication paths and types
- Power distribution system

Decisions to Be Made

☐ Facility Siting
☐ Security areas and layers of protection
☐ Targets and target locations
☐ Detection and assessment
☐ Access control system
☐ Delay mechanisms
☐ Response force capabilities

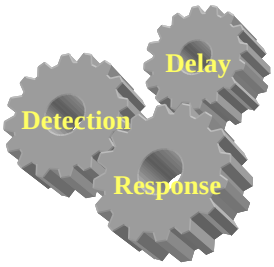
Module Summary

- Characterization involves gathering data that impacts the performance of the PPS such as:
    - Vital Areas
    - Physical Conditions
    - Operational Conditions
    - Non-Standard/Emergency Conditions
    - Physical Protection System
    - Infrastructure
    - Siting
- Siting greatly affects physical protection systems.

Module 8
Detection, Delay, and Response Overview

Module Objectives
After completing this module you should be able to do the following:

- Explain the three integrated components of Physical Protection System (PPS)
- Discuss the relationships between them
- Explain the characteristics of an effective PPS



Physical Protection Systems
System can rely on technology, guards, or combination to accomplish detection, delay, and response.

PPS Functions

Detection	Delay	Response
• Intrusion Detection • Access Control • Contraband Detection • Alarm Assessment • Alarm Communication and Display	• Passive Barriers • Active Barriers	• Guards • Response Forces

Security Event Sequence Example

A. Adversary begins attack.
B. Perimeter sensor detects an intrusion.
C. Security operator assesses the alarm as an intrusion and initiates response.
D. Response forces gear up and move to respond.
E. Meanwhile, adversary is making his way through the facility to his ultimate target.
F. He encounters more fences, distance, and barriers before getting to the building that has his target.
G. The adversary has a fake credential that he uses to attempt to tailgate an authorized employee through an access control point. The attempt fails, so he must attempt another means to enter or wait for another employee to try again.
H. Meanwhile, the security operator is tracking the progress of the adversary and communicating with response forces to direct them to the building.
I. Response forces intercept and apprehend the adversary outside of the building.

Questions

1. When does detection occur? _____
2. What are the delay elements? _____
3. Was the response timely? _____

Detection

Sensor activated → Alarm Signal Initiated → Alarm Reported → Alarm Assessed

Performance measures:

- Time for communication and assessment
- Frequency of nuisance alarms

A long time delay between sensor alarm and assessment lowers probability of detection

People can provide both an alarm and assessment simultaneously

An alarm without assessment is not detection

Delay

Providing obstacles to increase adversary task time

Examples: Physical barriers, response forces

Performance measure - Time to defeat obstacles

Delay (to be effective) must occur after detection

Response

Communicate to Response Forces → Deploy → Neutralize Adversary Attempt

Performance measures

- Time to communicate to response forces
- Time to deploy - gear up and travel to the adversary location
- Time involved in interrupting adversary activity through neutralization of the threat
- Probability of communication to response force
- Probability of deployment to adversary location
- Response force effectiveness

Part of the response may be the people who have detected the event

PPS System - Performance Measures

- Detection - Timely detection
- Delay – Time added to Adversary Task Time
- Response - Time, effectiveness

Relationship of PPS Functions

- System detection and response time must be less than adversary task completion time
- To increase the probability of system success
    - Detect intrusion earlier
    - Reduce assessment time
    - Increase adversary task completion time (add delay)
    - Reduce response time

Characteristics of an Effective Physical Protection System (PPS)

- **Timely detection and response**
- **Balanced protection**
- **Protection-in-depth**
- **Minimum consequence of component failure - Single-point of failure**
- **Secure by design**

Traditional Adversary Task Time vs. PPS Time Requirements

Relationship of PPS Functions

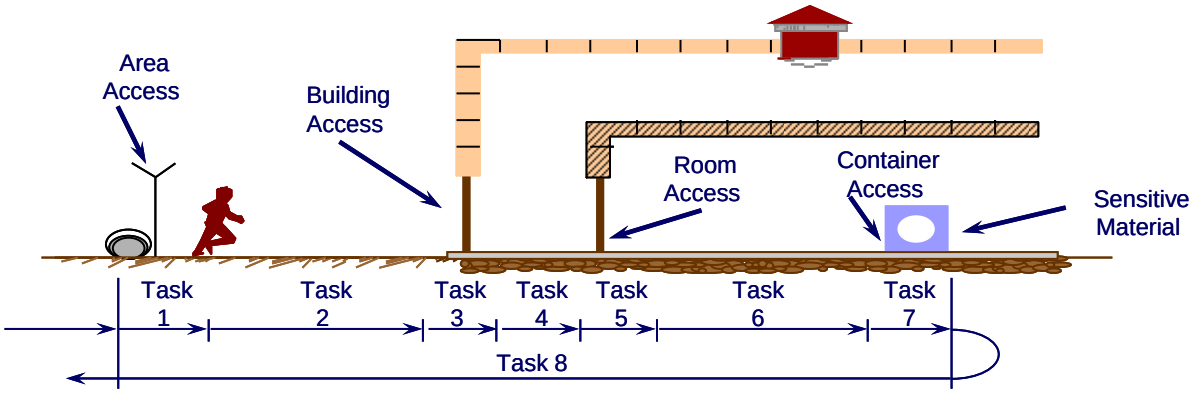
- System detection and response time must be less than adversary task completion time
- To increase the probability of system success
    - Detect intrusion earlier
    - Reduce assessment time
    - Increase adversary task completion time (delay)
    - Reduce response time

Characteristics of an Effective Physical Protection System (PPS)

- Security by design
- Protection-in-depth
- Minimum consequence of component failure or single-point failures
- Balanced protection
- Timely detection and response

Timely Detection and Response

For a successful system design, the total time for detection, delay, and response must be less than adversary task time to complete his or her goal



Protection-in-Depth

- Adversary must defeat or avoid a number of protection features in sequence
- Protection-in-depth should
    - Increase adversary's uncertainty about the system
    - Require more extensive preparations by adversary prior to attacking the system
    - Create additional steps where the adversary may fail or abort his mission

Balanced Protection

- No matter how an adversary attempts to accomplish the goals, effective elements of the PPS will be encountered
- Minimum time to penetrate each barrier is equal, and the minimum probability of detecting penetration of each barrier is equal
- Provides adequate protection against all adversaries along all possible paths
- Maintains a balance with other considerations such as cost, safety, structural integrity, operations, etc.

Minimum Consequence of Component Failure

- Contingency plans must be provided so that the PPS continues to operate after a component fails
- Redundant equipment can take over the function of disabled equipment in some cases; e.g., backup power exists if primary power is lost
- Some failures require aid from sources external to the facility such as:
    - National Guard is used to supplement security during times of higher alert status
    - Replace faulty sensors with manpower

Secure by Design - Security is

- Integrated into the site design process
- Essential to the mission of the facility
- Built into the system during construction

PPS Overview Summary

- PPS consist of
    - Detection
    - Delay
    - Response
- Characteristics of an effective PPS
    - Timely detection and response
    - Protection-in-depth
    - Minimum consequence of component failure
    - Balanced protection
    - Security by design
- The total time for PPS detection, delay, and response must be less than adversary task time to complete his or her goal

Infrastructure Development: Initiating a Physical Protection Program

Student Workbook

August 2010 Edition
Part 2

Module 9
Intrusion Detection

Module Objectives
After completing this module you should be able to do the following:

- Identify the role of Intrusion Detection in a PPS
- Discuss types of Intrusion Detection sensors
- Identify the performance characteristics of Intrusion Detection sensors
- Discuss characteristics of a good design

PPS Functions

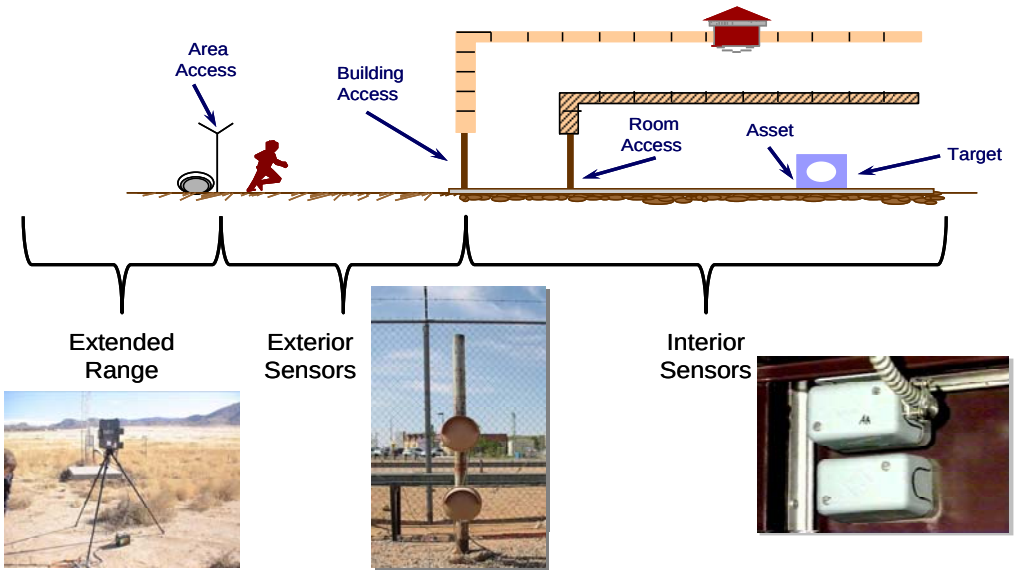
Detection	Delay	Response
• **Intrusion Detection** • Access Control • Contraband Detection • Alarm Assessment • Alarm Communication and Display	• Passive Barriers • Active Barriers	• Guards • Response Forces

Detection – a process that begins with sensing a potentially malicious or unauthorized act and completed with the assessment of the cause of the alarm

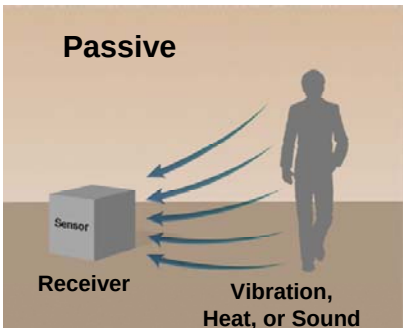
Detection Process

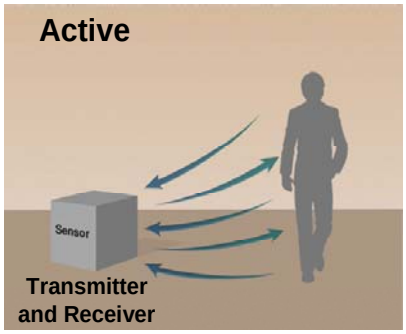
Sensor activated → Alarm Signal Initiated → Alarm Reported → Alarm Assessed

Types of Sensors

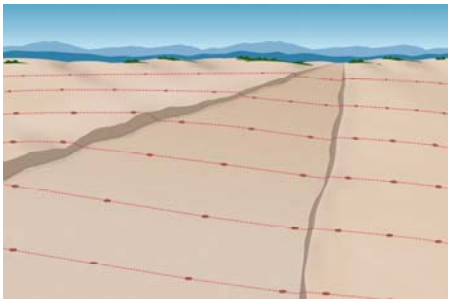


Sensor Features



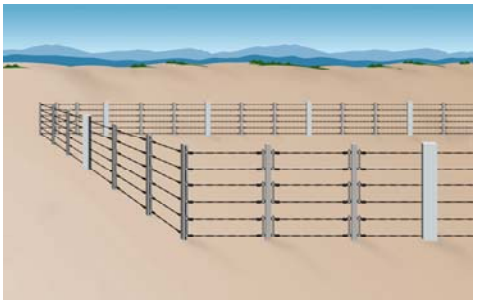


Covert



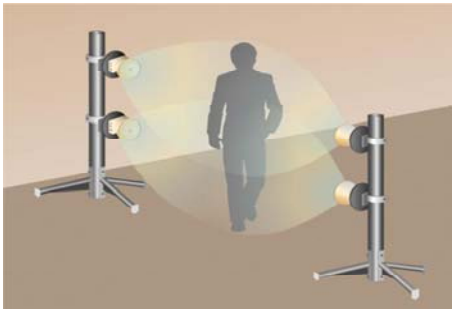
Sensors hidden from view
More difficult from intruder to detect

Visible



Sensors in plain view
Simpler to install and repair

Volumetric

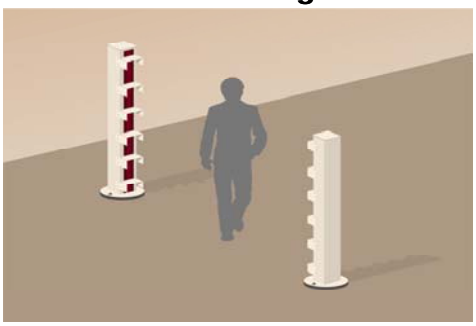


Detection in a volume of space
Detection volume is not visible

Line Detection

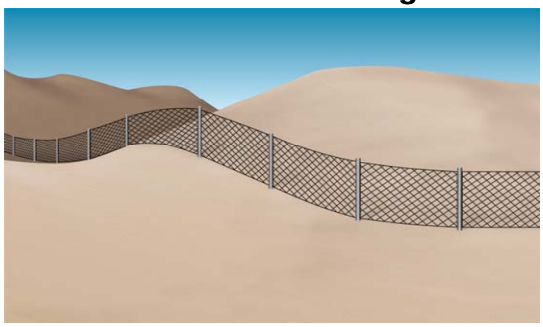
Detection along a line or plane
Detection zone easily identified

Line of Sight



No obstacles in the detection space
Requires flat ground surface

Terrain Following



Sensors detect over flat or irregular terrain

Types of Sensors

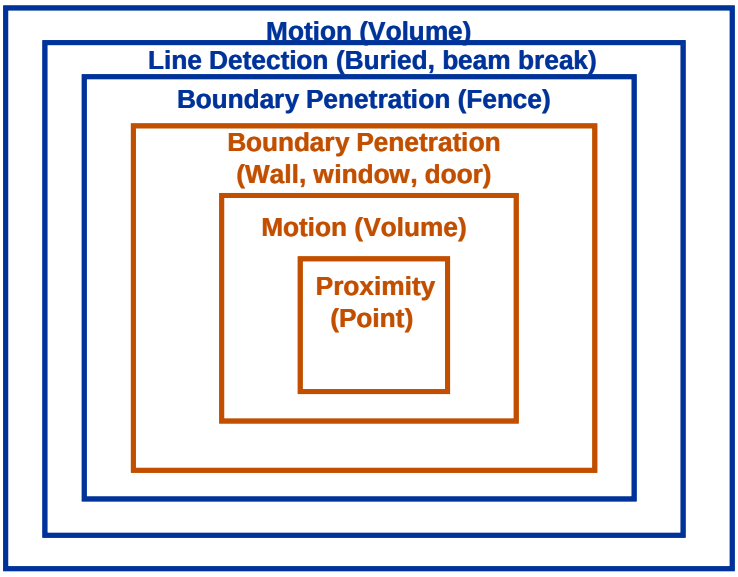
- Exterior sensors – used outside facilities and buildings
- Interior sensors - used inside building, entry points, and rooms housing targets
- Extended Range
    - Traditionally for early warning
    - Current applications: sense, assess, determine intent, and interdict adversary before reaching perimeter sensors

Characteristics of Intrusion Detection

- **Performance characteristics of Intrusion Detection**
    - **High probability of detection**
    - **Not vulnerable to defeat**
    - **Low Nuisance and False (i.e., unknown) Alarms**

- **High Probability of Detection - sensor location and selection that are highly likely to detect an intruder**
    - **Detection in Depth – multiple and complementary sensors**
    - **Site-specific System – sensor selection**
    - **Dependent on Adversary Capabilities**
    - **Use Performance Testing to Determine**

Protection-in-Depth



Exterior Sensor Applications **Interior Sensor Applications**

Environmental Dependencies

- Physical environmental conditions
    - Topography
    - Vegetation
    - Wildlife
    - Climate and weather

Environmental Dependencies (continued)

- **Industrial environment**
  - **Traffic**
  - **Noise – visual, sound, electromagnetic**

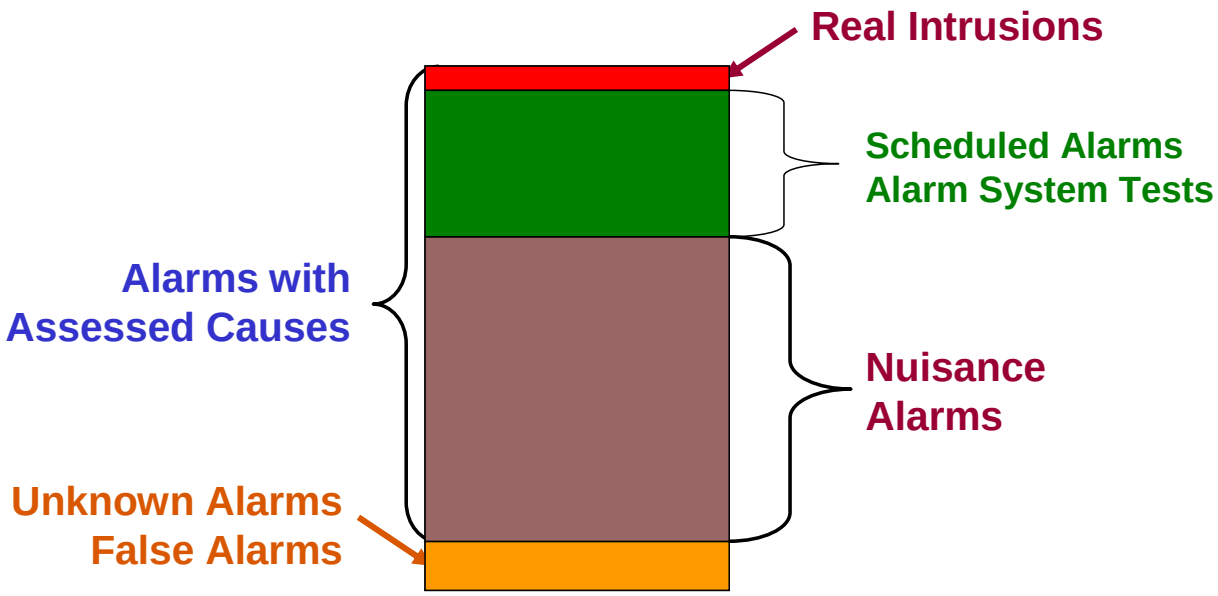
Site-Specific Dependencies

- **Site protection requirements – DBT**
- **Integration with Assessment System**
  - **Video capabilities**
  - **Response force**

Vulnerability to Defeat

- Adversary Tactics
  - Bypass: avoiding the detection volume of the sensor by crawling, jumping, tunneling, or bridging
  - Spoofing: tricking the sensor into not reporting an alarm
- Given proper knowledge, tools, and time, every sensor can be individually defeated

Performance Characteristics – Causes of Alarms



Categories of Alarms

- **Intrusion Alarm** – an alarm generated by an adversary intrusion
- **Scheduled Alarm** – an alarm generated by a scheduled test of a sensor
- **Nuisance Alarm** – an alarm generated by activity other than adversary intrusion or scheduled alarm where the cause is known such as wildlife, vegetation, weather
- **False Alarm** – an alarm generated and the cause is not known

Characteristics of Good Design

- High Probability of Detection
    - Detection in Depth
        - Layers of sensor detection
        - Multiple, detection at each layer
        - Combination of complementary sensors
        - Proper configuration of sensors
        - Clear Zone
- Minimal Vulnerability to Defeat
    - Integration with the barrier system
    - Continuous line of detection with overlapping detection zones
    - Protection of system and system components
    - Use of complementary and different types of sensors
    - Sensor selection for physical and industrial environment
- Integrated with Assessment System

Decisions to Be Made

- Siting of facility to facilitate detection systems
- Covert versus visible detection
- Performance test requirements
- Detection system requirements – exterior/interior
- Sustainability

Summary

- Intrusion Detection is one element of the PPS function of Detection and includes activation of the sensor and the initiation of the alarm signal.
- Types of sensors: exterior, interior, extended range.
- Performance characteristics include Probability of Detection, Vulnerability to Defeat, and the Nuisance Alarm Rate.
- A good sensor design has a high probability of detecting intruders with minimum of Nuisance Alarms

Module 10
Access Control Systems

Module Objectives

At the completion of this module, the student will be able to do the following:

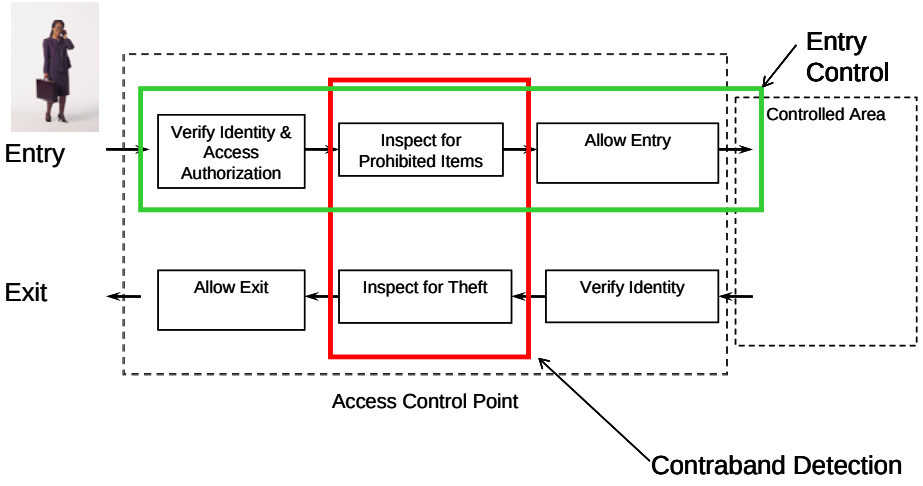
- Distinguish between access control, entry control, and contraband detection
- Identify 3 levels and three Types of Access Control
- Describe types of Contraband Detection
- Discuss Features of a Good Access Control System
- Describe Performance Measures

PPS Functions

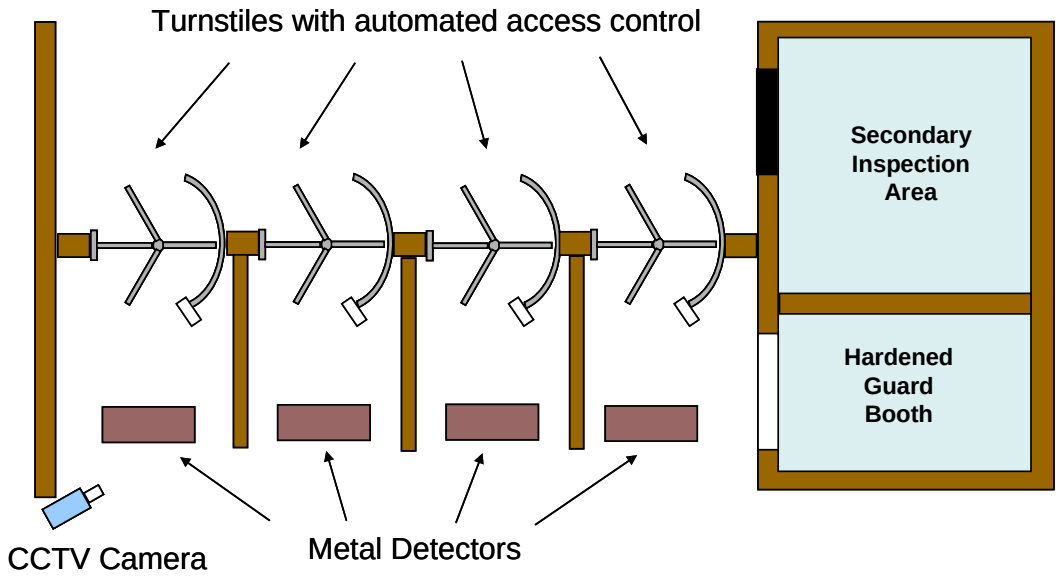
Detection	Delay	Response
• **Intrusion Detection** • Access Control • Contraband Detection • Alarm Assessment • Alarm Communication and Display	• Passive Barriers • Active Barriers	• Guards • Response Forces

Role of Access Control

- A perimeter security system provides a boundary around each protection layer to prevent or detect unauthorized penetrations.
- Access Control allows authorized persons and materials to move in and out through that boundary.
- Access Control must
  - Allow entry of authorized persons
  - Prevent entry of unauthorized persons
  - Allow exit of authorized persons



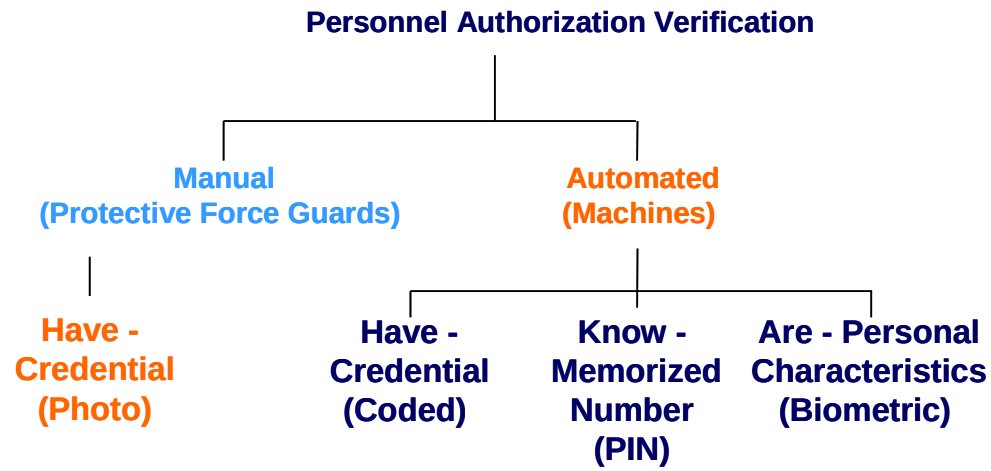
Access Control Techniques – An Example



Definitions for Access Control

- **Access Authorization** – an administrative determination that an individual is eligible
  for access to nuclear material or classified
  matter
- **Badge** - credential an individual is provided once access authorization is determined
- **Verification** – determination of access authorization
  at the entry control point
  - o Accepts authorized persons
  - o Rejects unauthorized persons

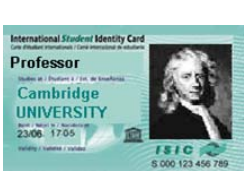
Types of Access Control – Verification Techniques



Types of Automated Access Control

Automated (Machines)

Have - Credential (Coded)	Know - Memorized Number (PIN)	Are – Personal Characteristics (Biometric)
• Photo badge • Exchange badge • Coded credential • Key	• Uniqueness of the PIN • Number of digits • System used to enter PIN	• Fingerprint • Hand geometry • Retinal pattern






Levels of Access Control – Verification Authorization

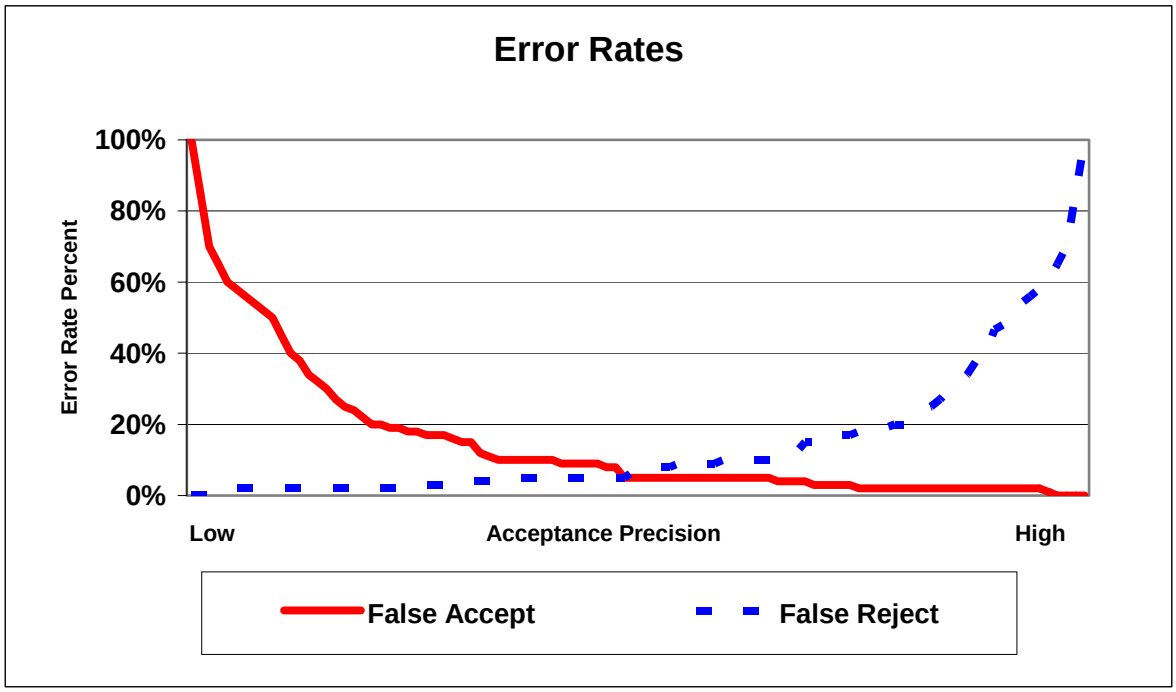
Level	Verification	Examples
1	One type	Credential OR PIN
2	Two Types	Credential AND PIN OR Credential AND Biometric
3	Three Types	Credential AND PIN AND Biometric

Features of a Good Access Control System

- Implements site requirements for limiting access per access authorization
- Integrated with Physical Boundary
- Personnel and Vehicle Entry
  - Blocks passage until access verification is complete
  - Provides secondary inspection and verification for specialty cases
  - Procedures for non-standard/emergency conditions
- Interfaces with Intrusion Detection System

Performance Measures of Access Control

- Throughput – measure of the time for an authorized person to successfully pass an entry or exit point
- Error Rates
    - Type 1 – False Reject (someone with authorization cannot get in)
    - Type 2 – False Accept (someone without authorization gets in)



Dual Role of Contraband Detection

Allow entry of authorized material	Prevent entry of • Weapons • Explosives • Other Contraband
Allow exit of authorized material	Prevent unauthorized exit (theft) of nuclear material

Definition of Contraband:
Contraband is any object that can be used by an adversary to gain an advantage in an attempt to remove, sabotage, or destroy a security target or do bodily harm.

Prohibited versus Controlled Items

- Prohibited – not allowed
- Controlled – allowed by certain people or under certain circumstances
    - Examples
        - Response force weapons
        - Radioactive sources for calibration of equipment
- Personally-owned vs. site-owned (business-use) items

Contraband Detection Inspections

People **Walk-through Systems**	**Things** **Package Inspection Systems**	**Vehicles** **Drive-through/Parked Inspection Systems**
Metal detection Backscatter X-ray scan mm- wave portal Trace explosives Radiation detectors	X-ray Trace explosives Radiation detectors Manual searches	Trace explosives Radiation detectors Manual searches

Decisions to Be Made

- Minimum number of access points for each protection layer
- Type of access control to be employed – technology, manpower, combination
- Adequate infrastructure to support access control
- Emergency situation management
- The need for contraband detection (entry/exit)
- Contraband materials list

Summary

- Access control limits the entry into and exit out of a site, facility, or area
- Entry control limits the flow of people
- Contraband detection detects entry and exit of unauthorized material
- Features of a good Access Control system include
    - Implements site requirements for limiting access per access authorization
    - Integrated with Physical Boundary
    - Procedures for non-standard and emergency conditions
- The Performance Measures for Access Control are throughput and error rates

Access Control Verification	Level of Access Control	Types of Contraband Detection
• What you have – credential • What you know – PIN • What you are – biometric	• Level 1 – credential **OR** PIN • Level 2 – credential **AND** PIN OR credential **AND** biometric • Level 3 – credential **AND** PIN **AND** biometric	• Persons • Packages • Vehicles

Module 11
Alarm Assessment, Communication, and Display

Module Objectives
At the completion of this module, you will be able to do the following:

- Describe the purpose of alarm assessment
- Identify two methods of alarm assessment
- Describe differences between assessment and surveillance

PPS Functions

Detection	Delay	Response
• **Intrusion Detection** • **Access Control** • **Contraband Detection** • **Alarm Assessment** • **Alarm Communication and Display**	• Passive Barriers • Active Barriers	• Guards • Response Forces

Detection Process

Sensor activated → Alarm Signal Initiated → Alarm Reported → Alarm Assessed

- Detection is the notification that a possible security event is occurring.
- Assessment is the act of determining whether the event is an attack or a nuisance alarm.
- *Detection is not complete without assessment*

Purpose of Alarm Assessment

- Determine the cause of each sensor alarm
  - Intrusion Alarm – threat
  - Nuisance Alarm – other assessed causes
  - False Alarm – undetermined causes
  - Scheduled Alarm – maintenance or test

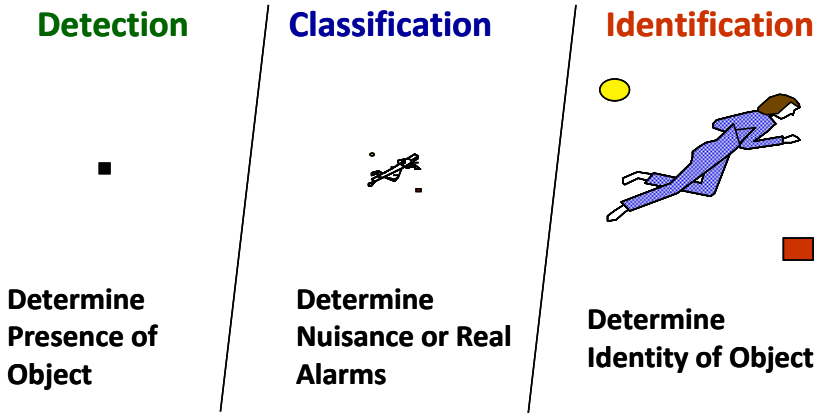
- Provide details for response – Who, What , Where , How Many

Methods of Alarm Assessment

Guard/Response Force	Video System Display
Elevated towers or roving patrols	Central Alarm station with stationary cameras or extended range cameras
Disadvantage: Delay between alarm and eyes on area for assessment	Disadvantages: • Cost of infrastructure and maintenance • Response Force assessment may still be required

Methods for Alarm Assessment

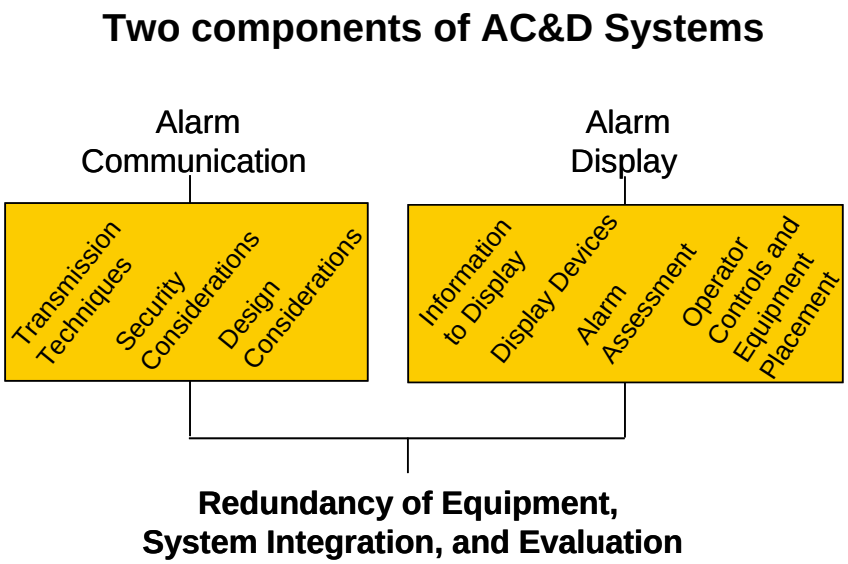
- **Alarm Prioritization**
  - Types
  - Simple static – sensors closest to asset given higher priority
  - Dynamic or groups of sensors – multiple alarms in one area given higher priority
  - Alarms and associated video displayed at CAS commonly displayed by priority and time
- **Resolution**
  - Resolution is the degree to which you can see fine details in viewed image
  - What you see depends on camera resolution, size of the object, contrast, and motion of the object.



Assessment/Surveillance

- **Assessment** – alarm-initiated video of a sensor detection zone at the time of an intrusion alarm
- **Surveillance** – continuous video monitoring of activity in an area without benefit of an intrusion sensor to direct attention to a specific event or area

Objectives of AC&D



Types of AC&D

- Simple system - Annunciator Panel with status lights or simple computer text/graphic display
- Complex system - Integrated systems with entry control, alarm system, and video system, networked to PC-based display system

Features of an Alarm Monitoring Station

- Provides overall status of site “Security System”
  - Alarm annunciation – audible and visual, location
  - Video displays
- Provides effective communication between CAS and Protective Forces
- Interfaces with Access Control
- Robust and reliable system
- Protection of system components and information
- Designed for ergonomics
  - Number of alarm monitoring station operators
  - Information management
    - Presents information quickly and effectively – maps, text, video playback
    - Logs information

Operator Functions of AC&D

- Start and end assessment of alarms – including video system control
- Initiate Response Force assessment or response to alarm
- Communicate information about alarm to response forces

Operator Functions of AC&D (continued)

- Non-alarm interface –
    - Entry Control
    - Access/Secure “strong rooms”;
    - Open/close buildings
    - Logging and Reports
- Monitor system status
    - respond to system outages;
    - report system degradation (i.e. burned out lights)

Decisions To Be Made

- **Assessment using technology or manpower**
- **Complexity of the alarm monitoring station**
- **Alarm prioritization**
- **Alarm control and display system specifications**
- **Resolution of video**

Summary

- Alarm assessment is to determine whether an alarm is a threat or nuisance alarm.
    - Detection is not complete without assessment.
- Alarm Assessment is either by Response Forces or Video Assessment.
- Video Assessment and Video Surveillance:
    - Assessment is alarm-initiated video display of a sensor detection zone.
    - Surveillance is continuous video display, which may or may not be observed at any given time.

Module 12
Access Delay Systems

Module Objectives

After completing this module you should be able to do the following:

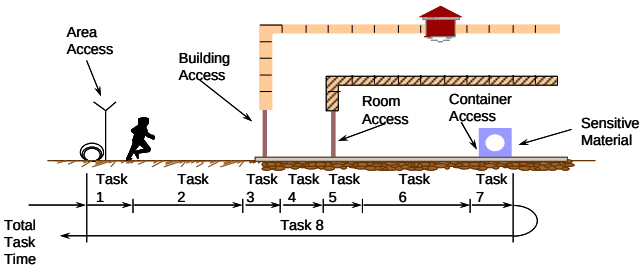
- Describe the purpose of Access Delay Systems
- Explain why detection must occur before delay
- List three characteristics of a good barrier design
- Recognize the definition of penetration

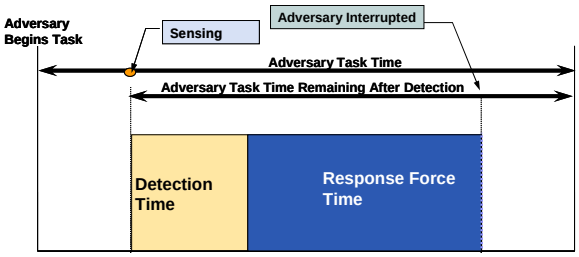
PPS Functions

Detection	Delay	Response
• **Intrusion Detection** • **Access Control** • **Contraband Detection** • **Alarm Assessment** • **Alarm Communication and Display**	• **Passive Barriers** • **Active Barriers**	• Guards • Response Forces

Purpose of Access Delay System

- Adversary must defeat or avoid a number of protection features in sequence.
- To be effective, delay must occur after detection.
- After detection, delay elements prevent completion of a malevolent act by providing delay until response forces can arrive.





Compensatory Measures

- Barriers must be considered in relation to the adversary's objective according to the DBT.
- Barriers must be in place 100% of the time, or compensatory measures must be taken.
- Compensatory measures include the following:
  - Personnel entry points: doors or turnstiles
  - Vehicle entry control point: Sally Port configuration (two barriers in series)
  - Vault door: provides added protection; must be guarded when open or accessed

Characteristics of Good Access Delay

- Provides Delay after Detection
- Exhibits a balanced design
    - No weak links
    - Considers all adversary paths, tools, and skills
- Employs defense-in-depth by delay-in-depth
    - Different defeat tools and skills
    - Multiple barriers
    - Different barriers

Definition of Penetration

- Penetration is when an individual can pass through, over, under, or around a barrier.
- Penetration times depend on the following:
    - Type of barrier
    - Location of the attack
    - Tools

Types and Principles for Access Delay

- Passive Barriers include structural elements:
    - Doors, walls, floors, locks, vents, ducts, and fences
    - Always fail secure
    - Conventional construction
        - Provides minimal delay against formidable threat; e.g., explosives
        - Can detain an adversary at predictable locations
    - Upgraded construction
        - Adds some delay
        - Design should maintain balanced protection
- Activated Barriers
    - Are not in place until activated by
        - guard
        - intrusion detection
        - combination
    - Include chemical fogs and smokes, foams, and irritants
    - Good for most types of threats
- Guards/Response Force
    - Flexible and continuous delay element
    - Provide minimal delay when adversaries use force except when in fixed and protected positions
    - Additional guards used in contingency plans

Decisions To Be Made

- On-site or off-site response determines the delay necessary
- Passive or activated barriers

Summary

- Access Delay System provides sufficient delay so the response force can arrive before the adversary completes a malevolent act.
- Features of good Access Delay:
  - provides delay after detection
  - exhibits balanced design without weak links
  - employs Delay-in-Depth
- Barrier penetration is when an individual can pass through, over, under, or around a barrier.
- Penetration time for the adversary will depend on the type and location of the barrier to be breached and the tools used for breaching.
- Delay elements include passive barriers, guards, and activated barriers.

Module 13
Response

Module Objectives
After completing this module, you should be able to do the following:

- Describe the Role of Response
- Distinguish between guards and response forces
- Discuss levels and strategies
- Describe the roles of command, control, and communication in successful response
- Discuss General Considerations for Response

PPS Functions

Detection	Delay	Response
• **Intrusion Detection** • **Access Control** • **Contraband Detection** • **Alarm Assessment** • **Alarm Communication and Display**	• **Passive Barriers** • **Active Barriers**	• **Guards** • **Response Forces**

Response follows Detection and occurs in parallel with Delay

Guards and Response Forces
Guard Forces - People that perform routine day-to-day duties such as alarm monitoring, escorting, administrative access control, routine patrolling, providing initial response.
Response Forces

- Persons responsible for the delay, interruption, and/or neutralization of an adversary to prevent an undesired event, such as theft or sabotage of nuclear material
- Persons, on-site or off-site who are armed and appropriately equipped and trained to counter an attempted unauthorized removal of nuclear material or an act of sabotage.

Considerations

- Staffing the guard and response forces
    - Direct or proprietary employees
    - Contract services
    - Use of technology
- Role of support agencies – written agreements
    - Radio frequency allocation
    - Off-site pursuit
- Legal do's and don'ts
    - Use of force
    - Hot pursuit
    - Arrest Authorities
- Contingency planning
    - Tactical planning
    - Absence and physical protection system failures
    - Additional duties of the guard force

Role for Response

Interruption – Successful arrival of the Response Force at an appropriate location to capture or detain the adversary. Requires:

- Accurate communication to response force
- Effective deployment of response force

Neutralization – Successfully stops the adversary before the adversary's goal is accomplished

- Response Force kills, captures, or causes the adversary to flee
- Use-of-Force continuum

Use-of-Force Continuum – the degree and circumstances for use of force

Presence → verbal → use of hands → less lethal → deadly force

Presence – Includes display of authority as a peace officer and such non-verbal means of communication as body language, demeanor, and manner of approaching.

Verbalization - Involves the direction, and commands given to the subject.

Intermediate Force – Hand-to-hand combat, restraining and detaining where an officer laying hands on a subject with the intention of gaining control of the subject. Examples include the use of a firm grip, escort position or grappling types of techniques designed to hold a subject down by using the weight of an officer's body. Also included in this level would be the application of temporary restraining devices such as handcuffs and leg restraints and the use of personal weapons such as hands, feet, elbows and knees to strike a subject.

Compliance Techniques: Includes joint manipulations, pressure point applications, take-down type techniques and the use of intermediate weapons in control type configurations.

Less-than-Lethal Tools – includes chemicals, tasers, and impact weapons designed to incapacitate a subject, but not kill him.

Deadly Force

- Used as a last resort when all other means have failed or use of deadly force is justified
- Includes the use of a firearm or any force which has a reasonable likelihood of causing death or serious physical harm.

Strategies

Four strategies for interruption and neutralization

- **Denial** – preventing adversaries from getting to an asset
- **Containment** – preventing adversaries from leaving the site with an asset
- **Recapture** – taking over by force a critical location on the site occupied by adversaries
- **Pursuit and Recovery** (contingency) – attempting to recover an asset removed from the site by adversaries

Aspects for Response

- Deployment of response personnel
    - Deployment is the action of initiating personnel response to confront the adversary and requires Planning, Training, and Practice
    - Response Force Equipment
        - Weapons – non-lethal and lethal
        - Personnel survivability– body armor, gas masks, chemical/biological suits, armored vehicles, fighting positions
        - Miscellaneous – night vision , flashlights, hand cuffs, load-bearing vest
        - Communication Equipment

- Communication with response personnel vital to command and control
    - Vital to command and control
        - Situational awareness
        - Duress
    - Multiple mechanisms for operations and contingency
        - Pagers
        - Phones – cell or land lines
        - Sirens and lights
        - Intercoms and public address systems
        - Computer terminals
        - Duress systems

Training

- General use of equipment – weapons, gear, communication systems and AC&D system
- Scenario-based – Guards and Response Forces for normal operations and contingency missions, understand tactics
- Sustained and dynamic – maintains awareness of conditions and changes and proficiency
- Performance-based testing using force-on-force exercises

Role of Command, Control, and Communication

- Command: Exercise of authority (decision making) by response force leaders
- Control: Direction by Response Force leaders over assigned personnel to accomplish the mission
- Communications: Allow real-time communication between the central alarm station, tactical leaders, and Response Force in the field and allow tactical leaders to direct the actions of the response based on adversary actions

Decisions to be made:

- Use of force
- Rules of engagement
- Guards versus response force responsibilities
- Types of communication
- Weapon systems and equipment
- Training
- Meets the DBT

Summary

- Response follows Detection and occurs in parallel with Delay.
- Guard Forces perform routine, on-site duties and Response Forces are responsible for interruption or neutralization of an adversary.
- The levels of force – use-of-force continuum ranges from presence to deadly force.
- The four strategies for interruption and neutralization are denial, containment, recapture, and pursuit and recovery.
- Communication is vital to command and control
    - Command – authority of response force leaders
    - Control – direction by response force leaders to response force
    - Communication – allows leaders to direct actions of the response based on adversary actions
- General Considerations of response functions are tactical Planning, Training, and Practice.

Infrastructure Development: Initiating a Physical Protection Program

Student Workbook

August 2010 Edition
Part 3

Table of Contents

Module 14
PPS System Evaluation

Module Objectives
After completing this module you should be able to do the following:

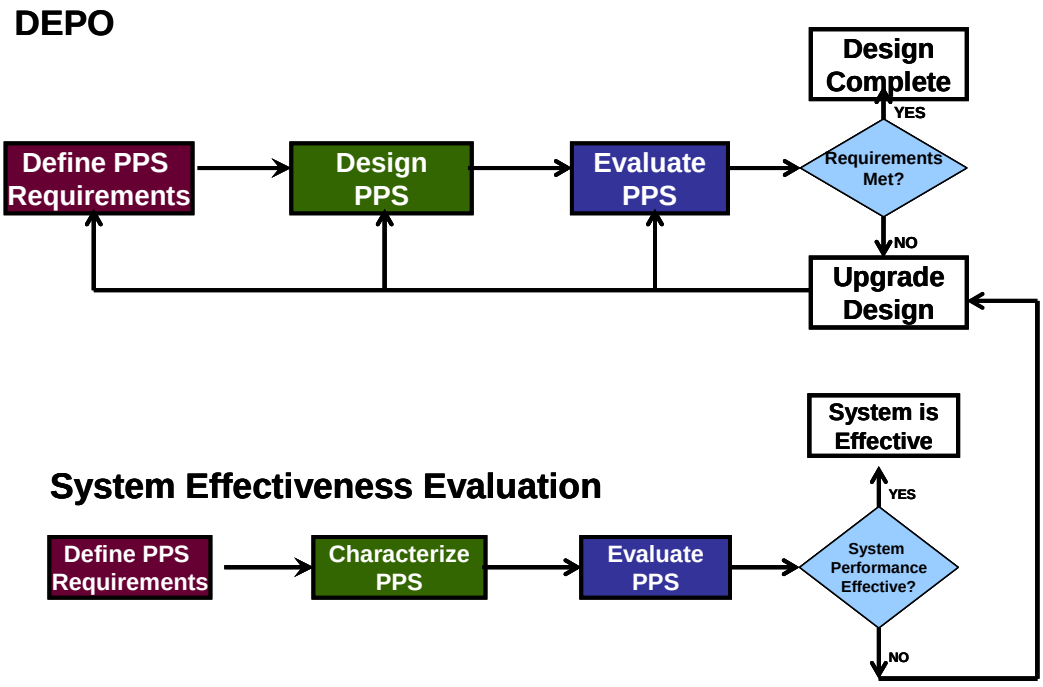
- Recognize the requirement for evaluation
- Describe the evaluation approaches
- Identify evaluation tools
- Describe two major factors that determine the quality of PPS performance evaluation

Relationship to INCIRC/225/Rev 5
4.4.2.4. To ensure that physical protection measures are maintained in a condition capable of meeting the State's regulations and of effectively responding to the State's requirements for physical protection, the State's competent authority should ensure that evaluations based on performance testing are conducted by operators at nuclear facilities and by shippers or carriers for transport. Evaluations should be reviewed by the State's competent authority, and should include administrative and technical measures, such as testing of detection, assessment and communications systems, and reviews of the implementation of physical protection procedures. When deficiencies are identified, the competent authority should ensure that corrective action is taken by the operator and by the shipper or carrier.

Evaluation Objectives
The Competent Authority and Licensees have complementary objectives for the evaluation of PPS:

- Meet regulatory and licensee requirements
    - Self-assessment by licensee
    - Inspection by competent authority
    - Periodic re-validation
- Verify and/or improve PPS performance
    - Verify PPS satisfies requirements
    - Identify system deficiencies
    - Analyze system upgrades
    - Compare cost versus performance
    - Select/implement overall best option

Design and Implementation Evaluation



Evaluation Approaches

- ***Expert:*** Performs PPS design and evaluation activities relying on personal knowledge and experience
- ***Prescriptive Approach:*** PPS design and evaluation based on specification and implementation of a required set of features
- ***Component Criteria Approach:*** standards approach to PPS design and evaluation that uses performance criteria for some security features
- ***System Performance Approach:*** A systems engineering approach to the design and evaluation of PPS based on specifying and achieving an overall system effectiveness against the Design Basis Threat (DBT) for theft and sabotage

Case Study: Evaluation of New Sensor
You have been approached by a vendor regarding a new type of sensor to consider for your physical protection system.

- How do you decide whether to use the sensor or not in your design?
- How do you understand the impacts to your existing system?

- Expert-based approach: a security expert might tell you in their opinion that it is desirable to have the sensor
  - How would you validate that opinion?
- Prescriptive approach: Requirement for a particular sensor type
  - Is this sensor part of the allowed sensor type?
  - How does the sensor perform in your particular environment?
  - What impacts does this sensor type have on the overall system performance?
- Component criteria approach: In this approach, there is a requirement to include required features that meet specific performance standard,
  - Example: "Probability of detection greater at the perimeter must be greater than 0.95 with a false alarm rate less than 1 in 10,000 alarms
  - How would you determine that sensor truly has that performance?
  - How would you know the impact of the sensor on the system performance?
- A system performance approach: Considers several issues in a disciplined approach:
  - Requirements:
    - What assets need protecting?
    - Who do these targets need to be protected from?
    - What level of protection is needed to protect the targets?
    - Are there reasons not to use the sensor?
  - Characterizing the PPS
  - Evaluating effectiveness
  - How do you answer the "buy or don't buy" question?
  - How do you validate your answer with the results of the analysis?

Performance-based Approach
Recall, from the risk management and regulatory requirements module, the performance approach:

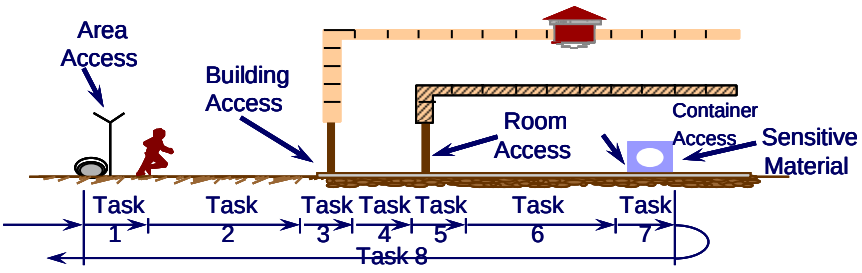
- The Competent Authority specifies the required level of system effectiveness, probability of effectiveness, against the DBT for the Licensee
- The Licensee complies by designing and evaluating its physical protection system to achieve this probability of effectiveness
- The Competent Authority is responsible for verifying that the Licensee's system satisfies the required performance against the potential adversary

Evaluation Tools

- Path Analysis – single/multipath
- Adversary Sequence Diagrams
- Scenario-based Analysis
- Exercises
  - Modeling/Simulation
  - Table Top
  - Force-on-Force

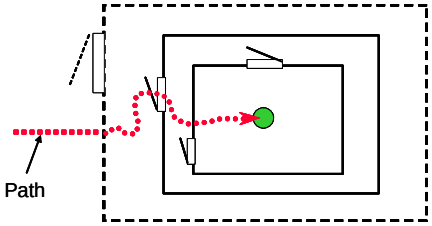
Adversary Sequence Diagram

Adversary Path: A time-ordered sequence of path elements, areas, and a target task that the adversary must traverse to complete an attack

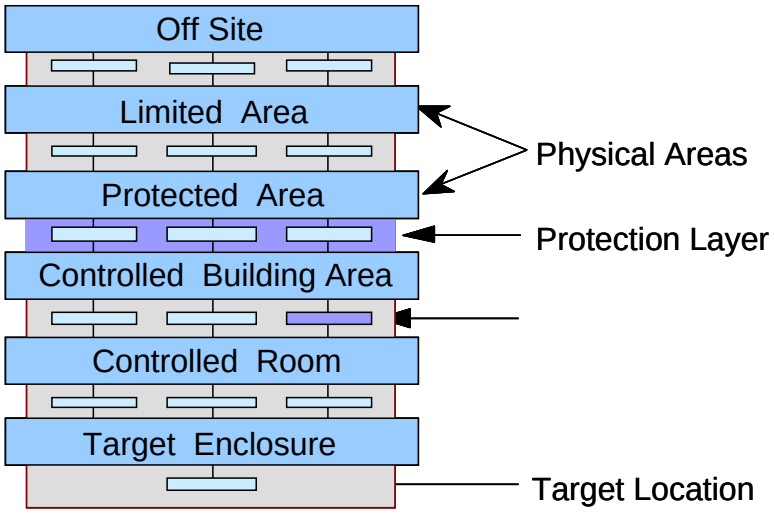


Metric – Total adversary task time

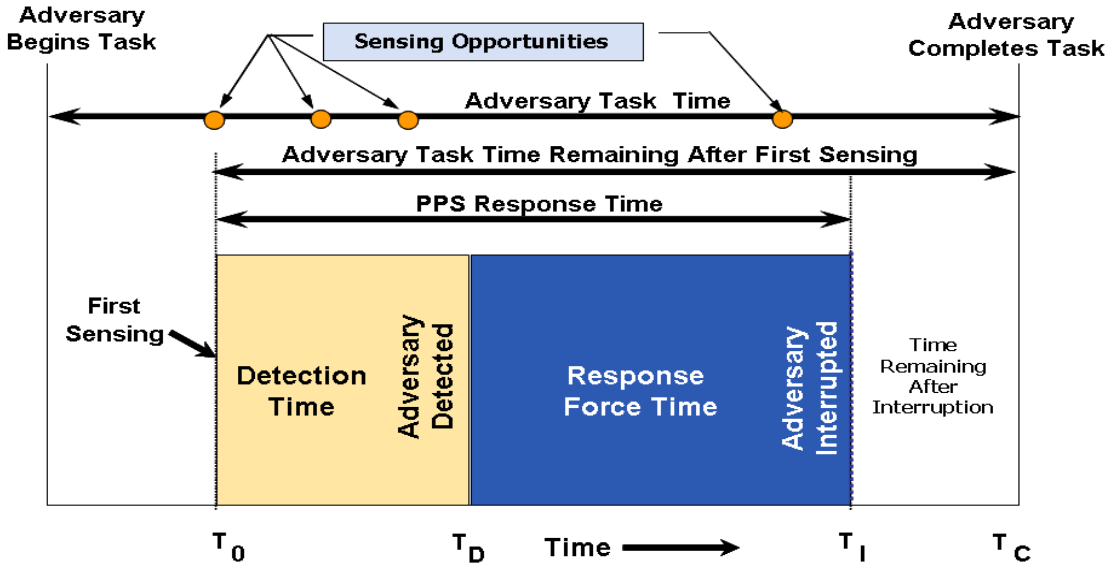
Concept of an Adversary Path
Path Analysis: An analysis using time-ordered sequence of path elements that examines the probability of detection and adversary task delay against the response force time



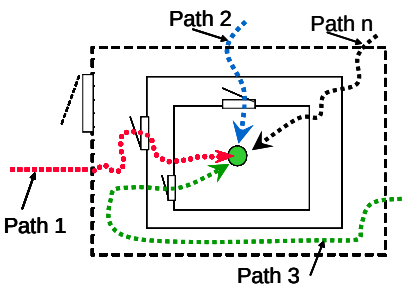
Concept of Adversary Sequence Diagram



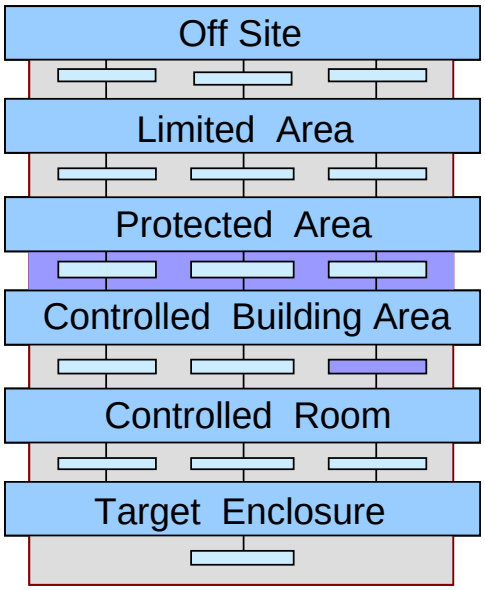
Path Analysis Uses Two Concepts
Adversary and PPS Timelines, discussed in the Design module, are used to calculate probability of interruption:



Multi-path Analysis
Determines whether detection and delay are sufficient along all adversary paths to provide an adequate level of Probability of Interruption, P_I, based on planned PPS Response Times



Developing a Scenario from a Path



Adversary Activities (Four adversaries)
Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during storm, last adversary monitors radio traffic.
Two adversaries penetrate door using burn bar, avoid sensor activation.
Two adversaries penetrate wall using linear shaped charge at night during storm.
Two adversaries destroy pump with linear shaped charge. All adversaries retreat.

Details of Scenario

Adversary	System	Response Force
Three adversaries drive up to gate in truck act as lost.	Normal procedures followed	Random Patrol in effect
Two adversaries surreptitiously generate a fence alarm then lie in wait to ambush patrol.		Unassessed alarm reported to patrol
The two teams coordinate an attack on the patrol and gatehouse.		Random Patrol ambushed near perimeter PN=0.2 Gatehouse guards attacked PN=0.3
The team of three set up ambush for secondary responders.		Secondary responder mobilize Secondary responders are ambushed probability of neutralization 0.50
Remaining adversaries proceed to storage vault and remove material.	Sensor's alarm	No forces available to respond

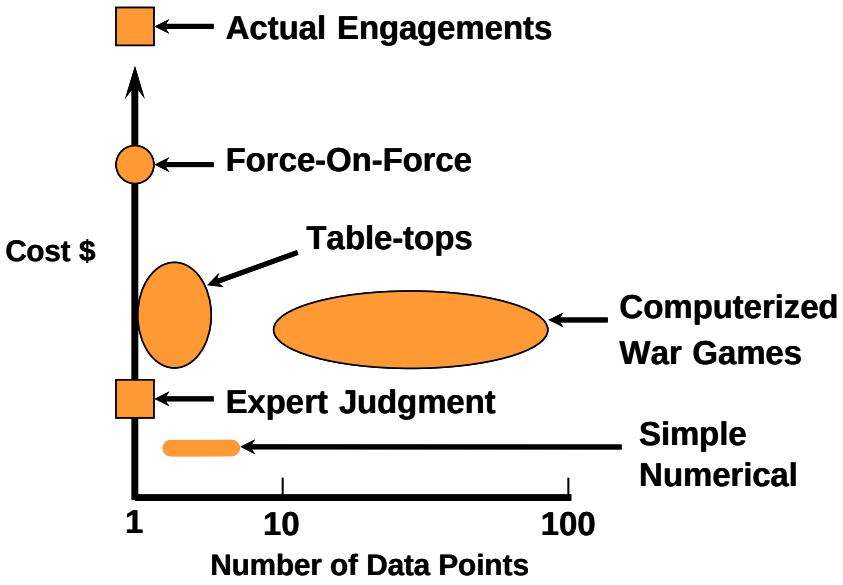
Scenario Evaluation

- System effectiveness is estimated considering the detection and delay at each of the scenario steps and the effectiveness of the response
- The team's expert opinion will be based on
  - Likelihood of detection achieved by the system
  - Duration of delay (after detection) being long enough for response to be effective
  - Ability of response to stop the adversary from achieving their goal if the response arrives in time

Exercises
Metric: Probability of Neutralization
Options

- Computer Combat Simulation Methodology
- Force-on-Force (FoF) Exercise Methodology (good at replicating individual behaviors)
- Tabletop Exercise Methodology (good at replicating decision-making)

Probability of Neutralization Cost



Evaluation Quality
There are two major factors that determine the quality of the PPS performance evaluation:

- Subject matter experts
  - Subject matter experts and their expert knowledge and experience are involved in the application of all evaluation methodologies
- Performance test data
  - Security component (detection, delay, and response) performance data used in the system evaluation must be high quality
    - Component performance data should be based on current performance testing

Decisions to be made

- Performance Criteria
- How to prove that system meets the criteria
- Evaluation approach
- Tools that will be used to validate performance
- Quality of evaluation

Summary

- INFCIRC/225/Rev 5 requires performance-based evaluation of physical protection systems

- Systems may be evaluated using expert, proscriptive, component, or system effectiveness approaches

- Evaluation tools include:
    - Adversary Sequence Diagrams
    - Path Analysis – single/multipath
    - Scenario-based Analysis
    - Exercises - Modeling/Simulation, Table Top, Force-on-Force

- Two major factors affecting evaluation quality are:
    - Subject matter experts and performance test data

Module 15
Transportation Security

Module Objectives
After completing this module, you should be able to do the following:

- Compare similarities and differences between fixed- site and transportation security
- Identify specific issues associated with transportation security
- Identify mitigating actions that can be taken
- Recognize the decisions to be made regarding transportation of nuclear and other radioactive materials

Transportation Elements

- Material movement within a site
- Material movement to and from a site

Differences

Property	Fixed Sites	Transport
Boundary	Fixed protection boundary	Moving boundary
Environment	Stable	Continuously changing
Control	Controlled	Uncontrolled
Predictability	Operations are predictable	Variation in schedule
Protection System	Fixed In place	Must be transportable

- Requires scenario analysis instead of a path analysis
    - Travel through public areas with no protected area
    - Constantly changing surroundings
    - Adversary attack and first detection both begin at the target

Similarities

- Follows the same design and evaluation process as for a fixed site
    - Determine system objectives
    - Characterize existing system in terms of Detection, Delay, Response
    - Analyze PPS

Transportation Conveyance Examples

- Tractor Trailer
- Railcar
- Ship
- Plane

Transportation Threat Examples

- Pirates
- Hijacking
- Ambush
- Sabotage

Transportation Detection, Assessment, Communication

- Detection
  - Outsider
    - Interior alarms
    - Response forces
  - Insider
    - Access control, includes 2-person rule
- Assessment and communications
  - Response force communicates alarm
  - Response force performs visual assessment

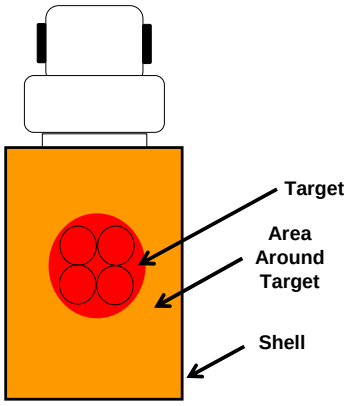
QUESTION: What makes working on your car time-consuming or difficult?

Transportation Delay Principles – Provide:

- Concealed delay features
- Keeping cargo secured to vehicle
- Forcing adversary to perform sequential tasks to gain access
- Forcing adversary to use many different tools to defeat delay features
- Creating difficult work area for the adversary
- Balanced delay

Delay Techniques

- Delay Techniques
  - Hardened vehicle
  - Interior hardening
  - Delay at asset
- Examples
  - Transporter
  - Doors and locks
  - Cages and tie-downs
  - Activated barriers



Transporter Example

- Multiple barriers provide more delay than single barriers
- Ballistics protection protects response forces
- Use hardened doors with locks such as electric, internal, or shrouded locks
- Cages and tie downs add delay as well as safety
- It is important to think through various scenarios and decide what elements of the transportation system need to be armored and which portions do not.

Activated Barriers May Be Applied in Transportation Security

- Exert minimum impact on operations
- Afford volume protection
- Offer multiple activation options
- Must provide adequate safety to personnel

Transportation Access Delay Considerations

- Constraints
  - Vehicle size and weight
  - Operational requirements
  - Standard vehicles provide minimal delay
- Delay Principles
  - Balance delay for all surfaces and all attacks
  - Use concealed delay features
- Adversary
  - Force adversary to perform sequential operations
  - Minimize adversary work area
  - Create difficult working environment for adversary
- Response
  - Consider insider issues in the design, use 2-person control
  - Need enough delay for response force to win

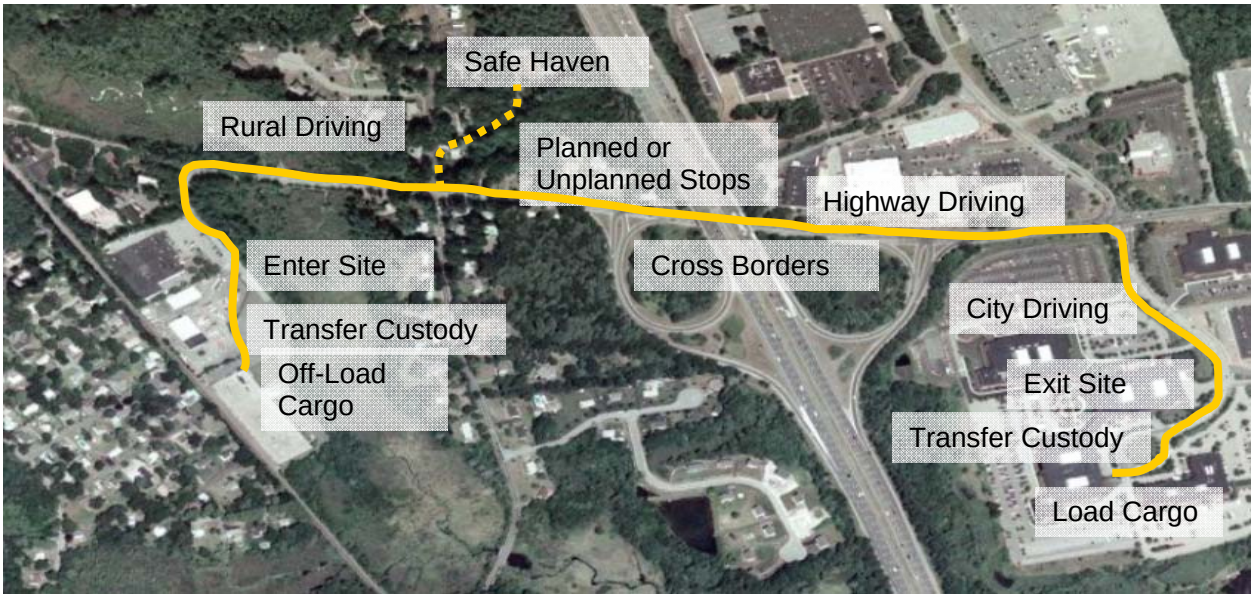
Access delay features should be present 100 % of the time or take compensatory measures

Transportation Response

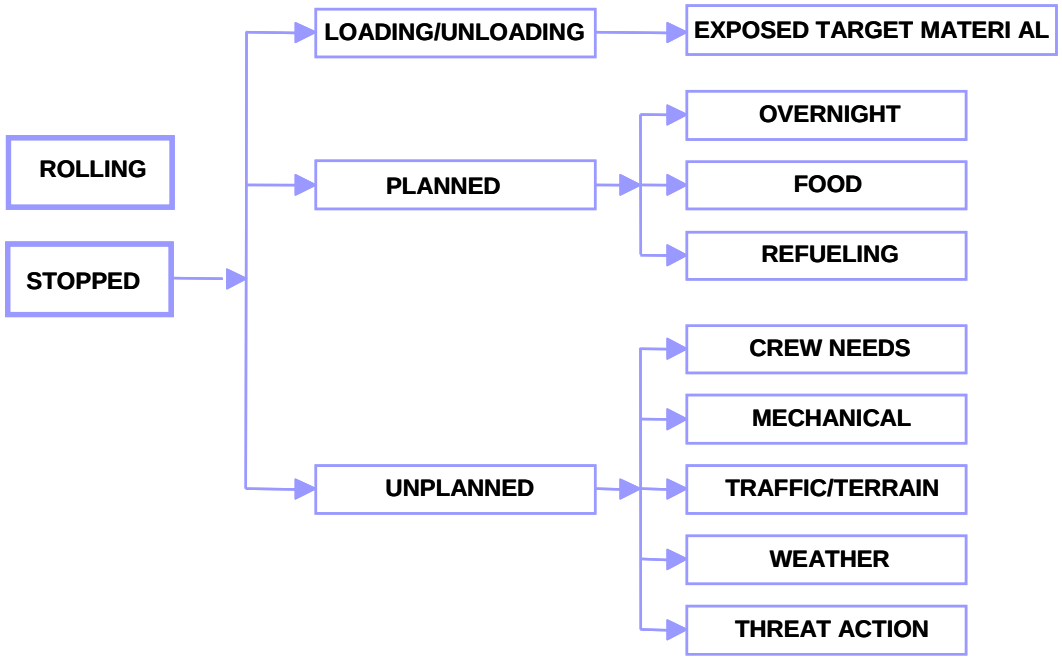
- Response force numbers, equipment, and training required depends on the threat
- Communications to
  - Each member of the response force
  - Secondary response force members
  - Transport control station
- Response Force configuration
  - Number of responders and their location relative to target
  - Secondary response force

Transportation Analysis

- Scenario analysis is most common tool
  - Vehicle states
  - Route surveys
- The scenario should be simple to carry out and consistent with the adversary's capabilities



Vehicle States



Possible Protection Actions

- Increase delay
- Enhance response force capabilities
- Vary routes and times
- Change location for scheduled stops
- Use look-alike shipments or decoys
- Dispatch covert shipments
- Use of high-profile shipments (military escort) or low-profile (civilian look-alike)
- Perform route surveillance reviews

Decisions to Be Made

- Processes for chain of custody
- Mode of transport
- Siting and routing transportation considerations
- Role and type of response

Summary

- There are both similarities and differences between fixed-site and transportation security
- Protection actions that can be taken include conveyance design, varied routing, and decoys
- Decisions to be made regarding transportation of nuclear and other radioactive materials
    - Mode of transport
    - Siting and Routing
    - Response

Module 16
Summary of Decisions to Be Made

Module Objective
At the end of this module, you should be able to identify the decisions that need to be made to initiate a Physical Protection Program

Nuclear Security Program Topics Covered
- Legal Framework
- Regulatory Framework
- Nuclear Security Programs
    - Physical Protection Program
    - Material Control and Accounting
    - Information Security
    - Personnel Security
- Physical Protection Systems
    - Requirements
    - Elements
    - Evaluation
- Transportation Security

Legal Framework Decisions - State
- Participation in international agreements
    - IAEA, NPT, Additional Protocol
    - Convention of the Physical Protection of Nuclear Material
    - Security Council Resolutions 1540 and 1373
    - International Convention for the Suppression of Act of Nuclear Terrorism
    - Code of Conduct on Safety and Security of Radioactive Sources
    - Guidance on the Import and Export of Radioactive Sources
- Designation of government agency(s) will be responsible for regulation of the physical protection for nuclear and radioactive materials and for working with the legislative body
- Identification of what nuclear and radioactive materials are permitted
- Identification of agency assigned to perform an intelligence-based threat assessment and determination on who how decisions will be made based on this threat assessment
- Select mechanisms for security transport of nuclear and other radioactive materials
- Response force responsibility and authorities

Regulatory Framework Decisions

- Develop a regulatory approach – Prescriptive, Performance, Combination
- Establish regulatory framework covering:
    - Licensing and evaluation of continued compliance
    - Definitions
    - Requirements
    - Considerations
    - Design Basis Threat
- Graded approach framework
    - Material categorization
    - Classification levels for the protection of information and materials
    - Levels of personnel trustworthiness

Nuclear Security Program Regulatory Decisions

- Physical Protection System
    - Define design and evaluation process
    - Evaluation criteria
- Material Control And Accounting
    - Determine material accounting system
    - Identify system requirements for material control
- Information Security
    - Determine process of certification and continued accreditation of information system
- Personnel Security
    - Identify a personnel identification system
    - Determine access and privileges levels

Licensee Physical Protection System Requirements Decisions

1. What needs to be protected?
    - Targets and target locations

2. What threats to protect against?
- DBT and local threat information

3. What level of protection is adequate?
- Performance criteria
- Evaluation processes and tools

Licensee Physical Protection System Design Decisions

- Facility Siting
- Security areas and layers of protection
- Detection and assessment for each layer of protection
- Access control system for each layer of protection
- Delay mechanisms for each layer of protection
- Guard/response force capabilities

Facility Siting

- Location Considerations
    - Population centers
    - Nearby businesses/structures
    - Nearest emergency response group
    - Security response force location
    - Availability and reliability of power and communications
    - Proximity to labor pool
    - Local crime
    - Wide-open spaces

- Environment Considerations
    - Topography at the site
    - Vegetation and wildlife
    - Background noise
    - Climate and weather
    - Soil conditions
    - Water flows/drainage

Protection Layers and Associated Security Areas

- Limited access areas
- Protected areas
- Inner areas
- Vital areas

Detection and Assessment Decisions

- Detection system requirements – exterior/interior
- Covert versus visible detection
- Assessment using technology or manpower
- Complexity of the alarm monitoring station
- Alarm prioritization
- Alarm control and display system requirements
- Adequate infrastructure to support detection and assessment systems
- Performance test requirements
- Sustainability

Access Control Decisions

- Minimum number of access points for each protection layer
- Type of access control to be employed – technology, manpower, combination
- Adequate infrastructure to support access control
- Emergency situation management
- The need for contraband detection (entry/exit)
- Contraband materials list

Delay Decisions

- On-site or off-site response determines the delay necessary
- Passive or activated barriers

Response Decisions

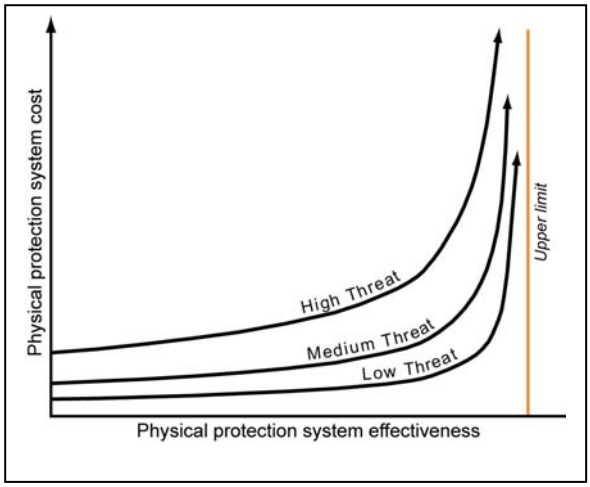
Location of forces – onsite/offsite, stations
Use of force
Rules of engagement
Guards versus response force responsibilities
Types of communication
Weapon systems and equipment
Training
Levels needed to meets the DBT

System Evaluation Decisions

- Performance Criteria
  - How to prove that system meets the criteria
- Evaluation approach
  - Tools that will be used to validate performance
- Quality of evaluation

Transportation Decisions

- Processes for chain of custody
- Mode of transport
- Siting and routing transportation considerations
- Role and type of response



Cost vs. System Effectiveness Decisions

- Siting
- Design of PPS
  - Detection
  - Delay
  - Response
- Cost trade-off

Summary

There are many decisions that must be made when designing a physical protection system for nuclear security applications for

- Fixed Sites
- Transportation

Module 17
Next Steps for Collaboration

Module Objective

- Summarize material covered
- Discuss future collaboration
- Determine next steps

Topics Covered

- Nuclear Security Roles and Responsibilities
- Supporting Regulatory Framework
- Physical Protection Systems
- Personnel Security
- Information Security
- Transportation Security

Cost vs. System Effectiveness

- Decisions that need to be made:
    - Siting
    - Design of PPS
        - Detection
        - Delay
        - Response
- Cost trade-off

Opportunities for Bilateral Collaboration

- Physical Protection Exchange Visits
- Site Assessments
- Technical Guidance
- Professional Training
- Best Practices Working Group

Professional Training - Regional or national training courses on

- Physical Protection of Nuclear Material and Nuclear Facilities
- Security of Research Reactors
- Foundations of Physical Protection
- Design Basis Threat (DBT)
- Protection against Sabotage
- Vital Area Identification
- Insider Threat
- Nuclear Security Culture
- Initiating a Physical Protection System Practical 5-Day Course

Next Steps

1. What types of collaboration would you like to pursue?

2. Who would be the point of contact?

3. What would be the venue?

4. What access would be required?

Summary

- This was only an introduction to physical protection.
- States must provide a legal and regulatory framework for physical protection.
- Every element of physical protection has effectiveness versus cost trade-offs.