SAND2008-2024C

Basic Security Principles

Presented by Roger S. Case Jr., PhD.

Training Course on Protection Against Nuclear Terrorism: Security of Radioactive Sources

Riyadh, Saudi Arabia—April 2008

IAEA
International Atomic Energy Agency

Objectives

After this session, participants should be able to:

- Identify the elements of security systems
- State the purpose of physical protection
- State the three essential questions that define the requirements for a PPS
- State the functions of a PPS
- Explain the principle of timely detection
- Recognize the need for security management functions and measures

IAEA

Elements of a Security System

- Physical protection system
  - Deter adversary from attacking
  - Defeat adversary if he does attack
- Security management
  - Ensure that the physical protection system functions properly
  - Includes measures such as verifying trustworthiness of employees and protecting sensitive security information

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

Three Essential Questions that define the requirements for a PPS

1. What must I protect? (What is the target to be protected?)

2. What must I protect against? (What is the threat against which the PPS must be designed?)

3. What level of protection is adequate? (What is the acceptance criteria for the PPS?)

1. What must I protect?

Radioactive sources

2. What must I protect against?

- The regulator or the operator must define a threat that the physical protection system is expected to withstand
- The defined threat specifies the adversary attributes and characteristics that the PPS must be designed to defend against

The Value of a Threat Definition

The threat definition provides a rational basis for:

- 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

IAEA

Categories of Threats

- External Threat
  - Protestors, Terrorists, Criminals
- Internal Threat
  - An Insider is anyone with authorized, unescorted access who could
    - Act alone or in collusion with external threat
    - May be passive or active
    - May be violent or nonviolent

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 w/ Insider
  - Support Structure

3. What level of protection is adequate?

- Objective: reduce the risk associated with use of a source to an acceptable level
- Must strike a balance between physical protection and beneficial use
- The level of security should reflect the potential consequences of misuse of the source: higher potential consequences imply higher levels of security

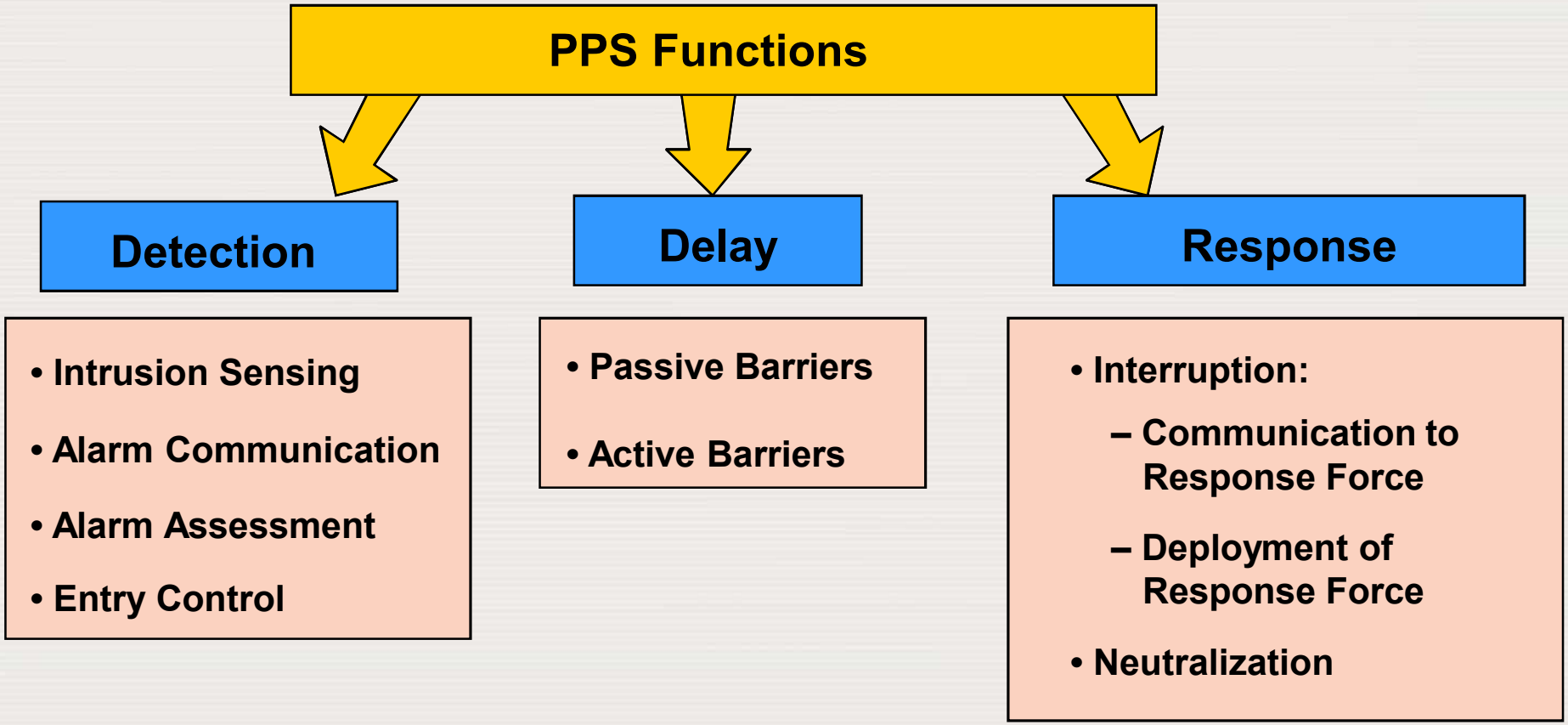
Graded Physical Protection Requirements

- The level of protection required for a source should be commensurate with the potential consequences that might result from misuse of the source
- Graded security measures should also consider:
  - Anticipated threat
  - Relative attractiveness of the source to the threat
  - The need for beneficial use of the source

Physical Protection System Objective: Prevent Theft and Sabotage

- Deter the Adversary
  - Implement a PPS which all adversaries perceive as too difficult to defeat
  - Problem: deterrence is impossible to measure
- Defeat the adversary with PPS
  - PPS functions required: detection, delay, response
  - Actions of response force prevent adversary from accomplishing his goal

PPS Functions



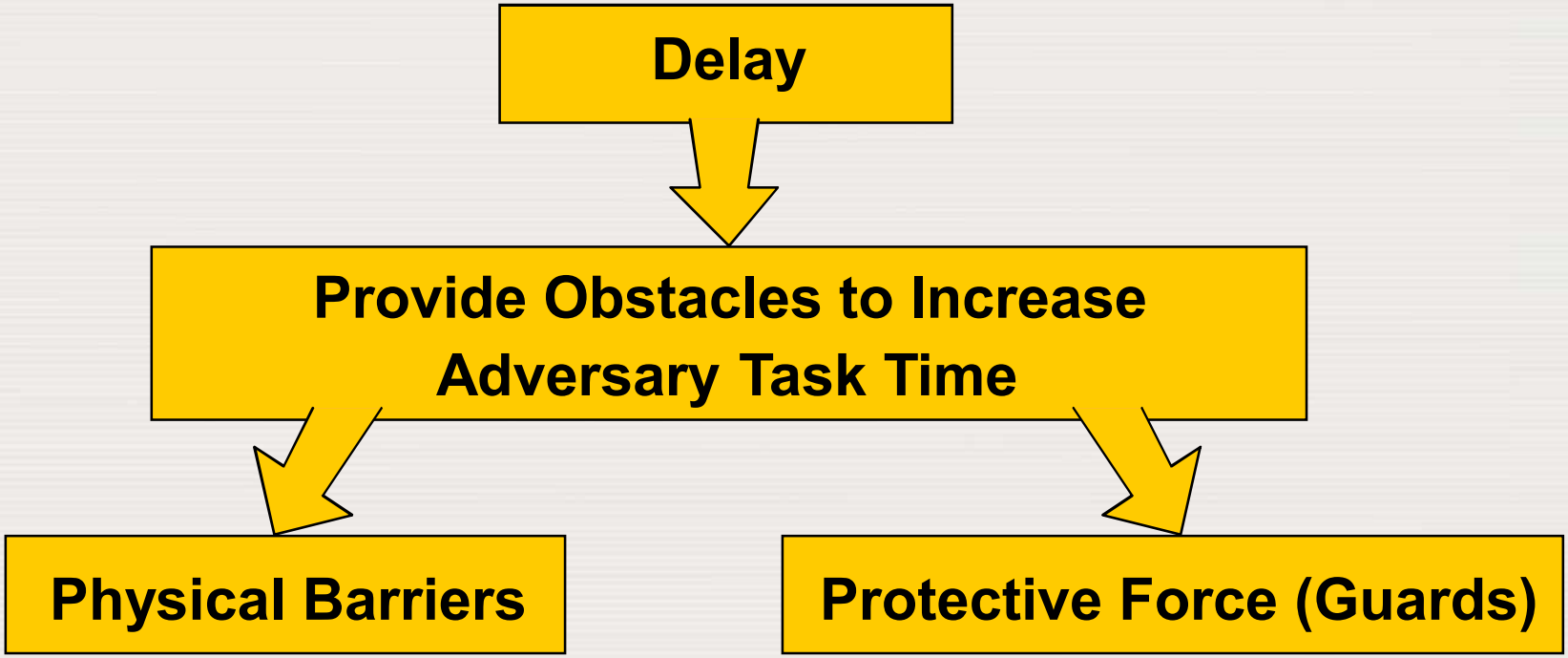
Detection

Performance Measures:

- Probability of Sensor Alarm (P_S)
- Time for Communication and Assessment (T_C)
- Frequency of Nuisance Alarms (NAR)
- Probability of Assessment (P_A)
- $P_D = F(P_S, T_C, NAR, P_A)$

IAEA

Delay



- Performance Measure: Time to Defeat Obstacles

Response

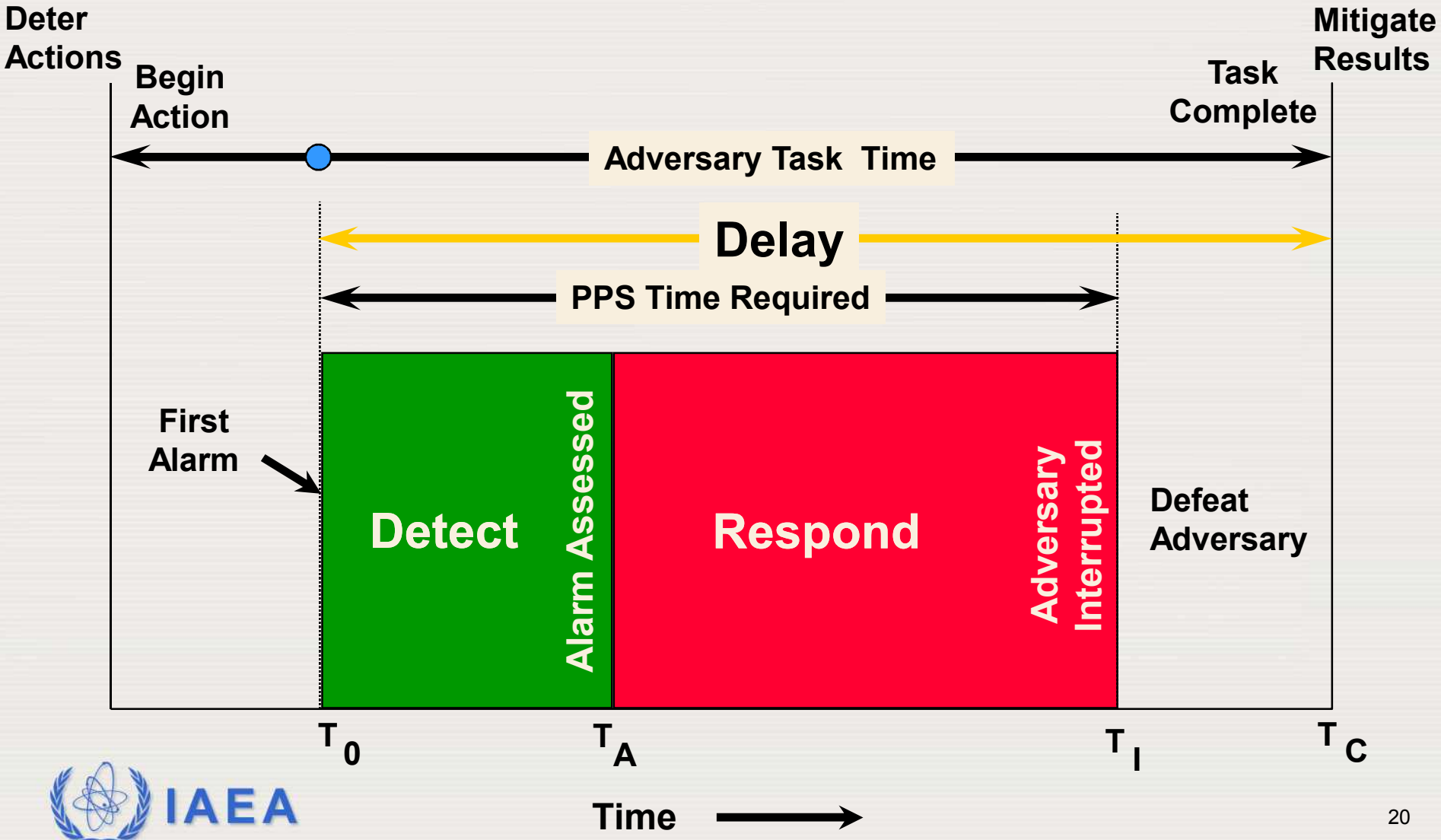
- Performance measures
  - Probability of communication to response force
  - Time to communicate
  - Probability of deployment to adversary location
  - Time to deploy
  - Response force effectiveness

Physical Protection System Effectiveness

In order to be effective in preventing malicious acts, the three PPS functions must work together to:

- Interrupt the adversary before he completes his tasks (timely detection)
- Neutralize the adversary (effective response)

The Principle of Timely Detection



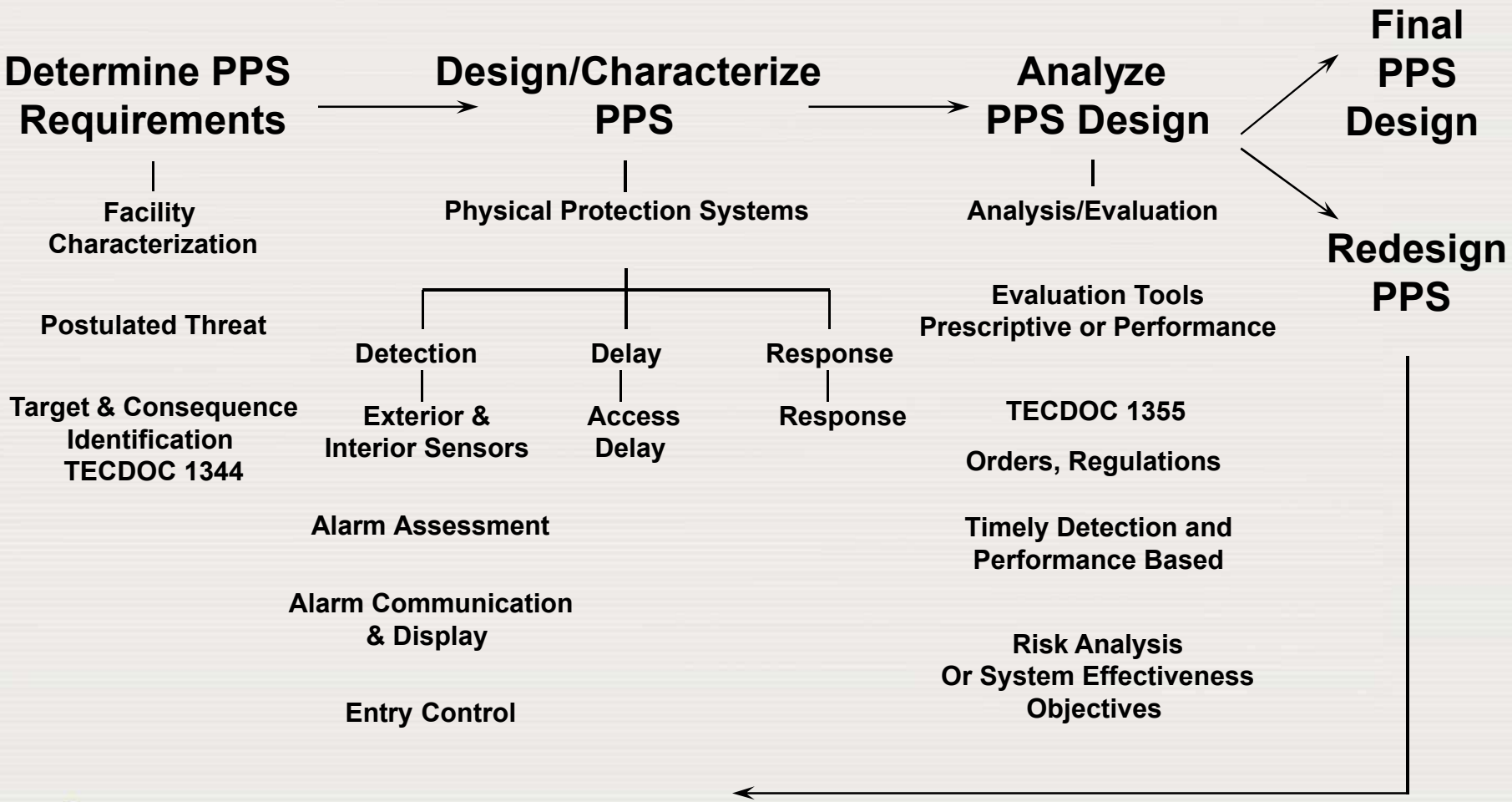
Interaction with Outside Response Agencies

- Written agreement or understanding
- Key issues for consideration
  - Role of support agencies
  - Communication with support agencies
  - Off-site operations
- Joint training exercises

Characteristics of an Effective Physical Protection System

- Defense-in-depth
  - Series of detectors better than a single one
  - Prefer to use complementary sensors that use different principles
- Balanced protection
  - Does not create an easy path for adversary
  - Applies to Detection as well as Delay
- Sufficient protection but not too much
  - Enough Detection, Delay, and Response
  - Meet the “System Effectiveness” criteria
- One feature can compensate for another's weakness

Physical Protection Fundamentals: Design and Evaluation Process Outline (DEPO)



Key Security-Related Provisions of the IAEA Code of Conduct

1. Sources should be **protected** against malicious acts
2. States should define their **domestic threat**
3. States should assess the **vulnerability** of its radioactive sources
4. Legislation and regulations should have requirements for **security measures**
5. Regulatory bodies should establish requirements for **security management**

Implementing Security Measures for Radioactive Sources – TECDOC 1355

Implementing Security Measures Using TECDOC 1355

- Establishes four Security Groups based on the level of risk associated with misuse of sources
- Assigns sources to Security Groups based on the source category
- Defines performance objectives for protection of each Security Group
- Identifies administrative and technical measures that can be used to meet the performance objectives

Security Management

Security Management Objective

- A physical protection system combines detection, delay, and response measures to achieve the required level of system effectiveness against the identified threat
- A complete security program also requires security management measures which help ensure that the physical protection system functions properly

Typical Security Management Measures

- Security plan
- Contingency plan
- Information security
- Reliability and trustworthiness of personnel
- Security culture
- Inventories and records
- Reporting of security incidents

Presentation Objectives

After this session, participants should be able to:

- Identify the elements of security systems
- State the purpose of physical protection
- State the three essential questions that define the requirements for a PPS
- State the functions of a PPS
- Explain the principle of timely detection
- Recognize the need for security management functions and measures

IAEA

Summary

- The purpose of a physical protection system is to prevent malicious attacks (theft or sabotage)
- Fundamental PPS questions:
  - What must be protected?
  - What must it be protected against?
  - What constitutes adequate protection?
- Prescriptive or performance-based approaches can be used to demonstrate that security objectives are met

Summary (2)

- The essential functions of a physical protection system are Detection, Delay, and Response
- Timely Detection – the adversary task time following detection must be longer than the response force time
- Security management measures are needed to ensure that the physical protection system functions properly

Nuclear Security Culture

Presented by Roger S. Case Jr., PhD.

Training Course on Protection Against Nuclear Terrorism: Security of Radioactive Sources

Riyadh, Saudi Arabia—April 2008

IAEA

Learning Objectives

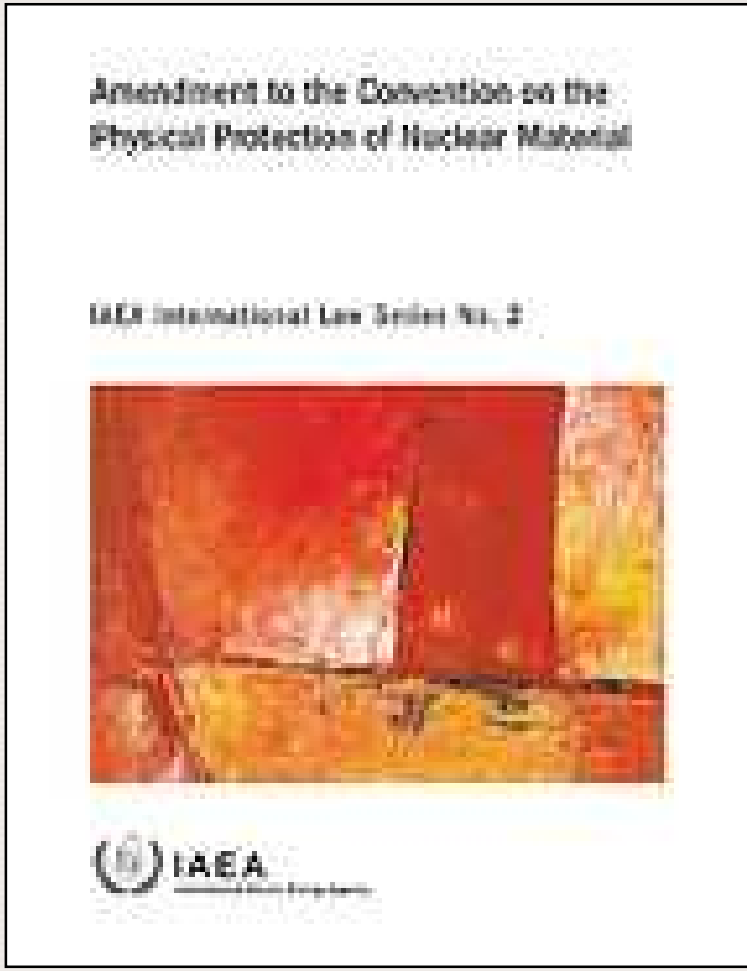
- Recognize the key provisions of the IAEA Implementing Guide on Nuclear Security Culture
- Describe the model of nuclear security culture used in the IAEA Implementing Guide
- Outline the characteristics of a strong nuclear security culture

IAEA

Fundamental Principles

- Incorporated in Amendment to the CPPNM, July 2005
- Fundamental Principle F - Security Culture:

  "All Organizations involved with implementing physical protection should give due priority to the security culture; to its development and maintenance necessary to ensure its effective implementation in the entire organization".



IAEA

Extension to Radioactive Sources

- **Code of Conduct on the Safety and Security of Radioactive Sources (2003)**

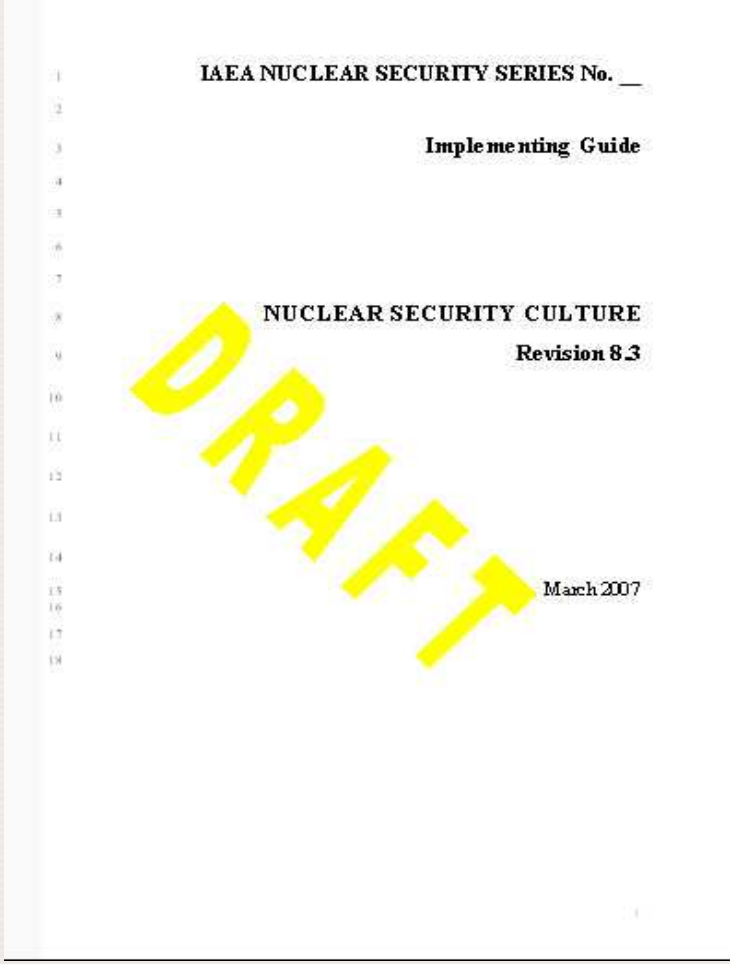
  "Every State should . . . ensure:

  (b) the promotion of safety culture and of security culture with respect to radioactive sources."

IAEA

IAEA Definition of Nuclear Security Culture

- From IAEA Implementing Guide Section 2
  - "The assembly of characteristics, principles, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security".
  - "Appropriate Nuclear Security Culture ensures that the implementation of nuclear security measures receive the attention warranted by their significance".


IAEA NUCLEAR SECURITY SERIES No. __

Implementing Guide

NUCLEAR SECURITY CULTURE

Revision 8.3

DRAFT

March 2007

IAEA

Scope of the IAEA Implementing Guide

- **Defines basic concepts and elements of nuclear security culture**
- **Provides an overview of the attributes of nuclear security culture**
- **Emphasizes that nuclear security ultimately depends on individuals**
  - Beliefs and attitudes are the basis
  - Stated principles guide behaviour
  - Management systems and individual behaviour can be seen and evaluated

IAEA

Nuclear Security Framework

- Nuclear Security includes a range of elements:
  - Legislation and regulation
  - Assessment of the threat
  - Management systems at facilities
  - Hardware systems at facilities
  - Deterrence and mitigation activities

- The entire nuclear security framework depends on people
- This is called the “human factor”

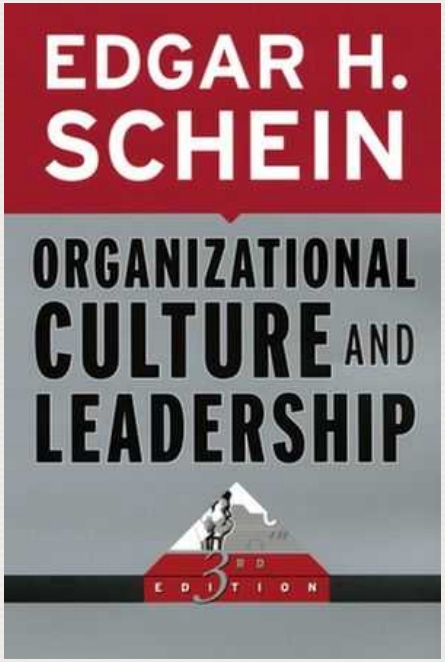
IAEA

Basis for Nuclear Security Culture

- Edgar Schein Model of "Organizational Culture and Leadership" (1997)

- Layers range from invisible and non-measurable to visible and measurable
  - Visible layers have performance indicators
  - Must infer what is invisible from the visible

- Bottom layer is the base for other characteristics (invisible)
  - Credible threat exists
  - Nuclear security is important



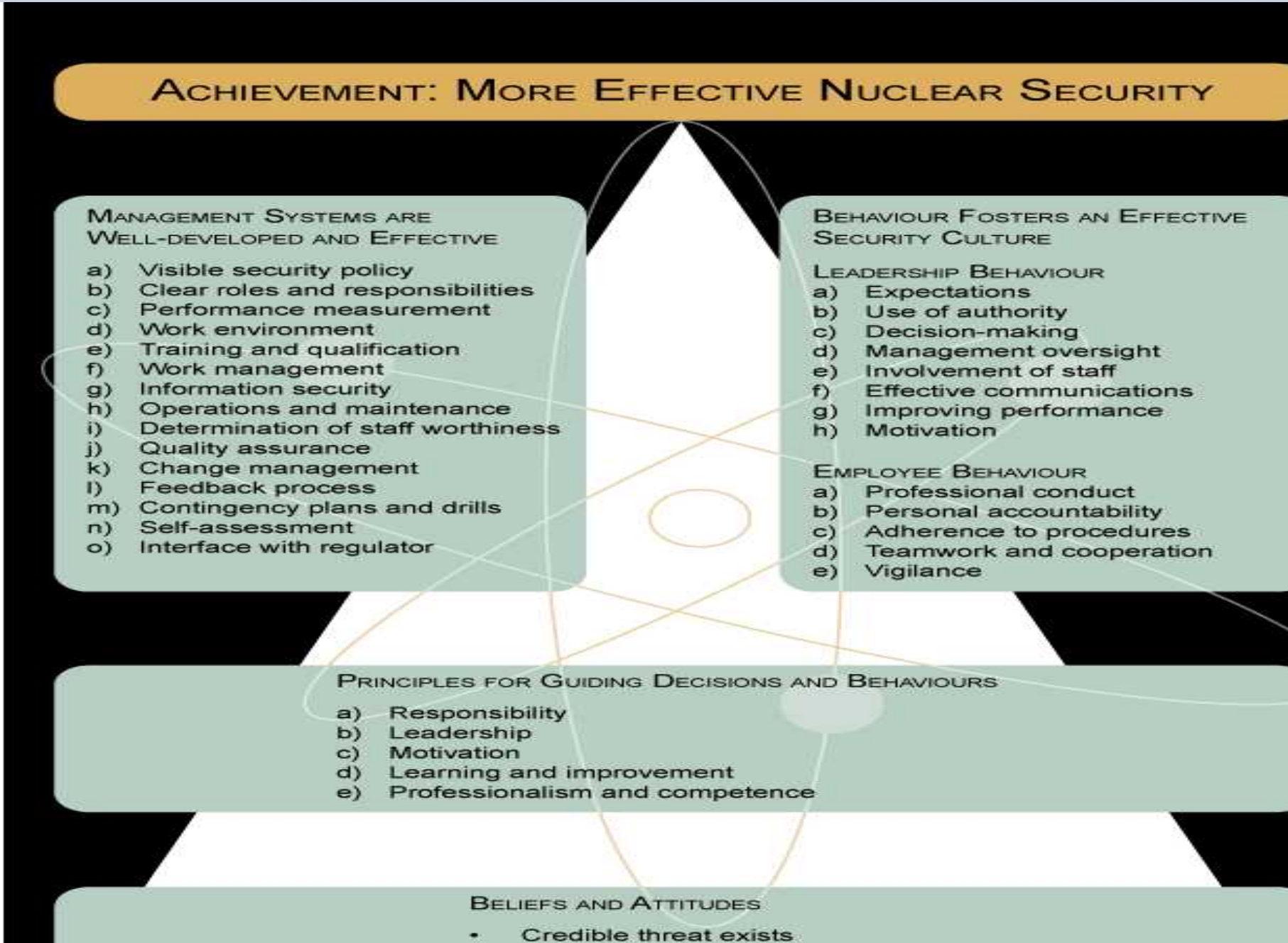
IAEA

Characteristics of Nuclear Security Culture

- Beliefs & Attitudes
- Behaviour
- Principles for guiding decisions and behaviour
- Management systems

IAEA

Nuclear Security Culture Model



Characteristics of Nuclear Security Culture

- Characteristics listed in the model:
  - Cannot be comprehensive
  - Not applicable in all circumstances
- Characteristics should:
  - Encourage self-examination
  - Be thought provoking rather than prescriptive
- Indicators of characteristics are:
  - Not comprehensive
  - A starting point for self-evaluation

IAEA

Role of the International Community

- Common interest of States in nuclear security
- International community provides guidance in security areas
- International community facilitates bilateral, multilateral or international assistance programmes
- The IAEA in particular offers many publications, training and assistance programs in nuclear security

IAEA

Role of the State

- Establish legal and regulatory framework to foster effective nuclear security culture

- State organizations may involve:
  - Nuclear regulator
  - Law enforcement
  - Military
  - Health ministries
  - Intelligence organizations
  - Emergency response authorities
  - Public information officials

IAEA

Role of the State

- State establishes security policy
  - Should be based on current threat
  - Determines security requirements
  - Good nuclear security culture requires good policies
- State establishes legal framework
  - Penalties for violation
  - Protection of sensitive information
  - Trustworthiness determination requirements
- State distributes and coordinates responsibilities
  - Coordination among facilities
  - Typically the nuclear regulatory authority is focal point
- State runs coordination mechanisms
  - Good coordination leads to good nuclear security culture

IAEA

Role of Organizations

- Within a State, various organizations have responsibilities for nuclear security:
  - Users of radioactive sources
  - Operators of nuclear facilities
  - Transporters of nuclear materials
- Each organization in the State should have:
  - Organizational nuclear security policy
  - Management structure well defined
  - Necessary resources to do their job
  - Management systems to effect nuclear security
  - Conduct review and improvement efforts
- Organizations operate under the State systems
  - Nuclear security culture is seen in operation at the organization level

IAEA

Role of Managers in Organizations

- Managers
  - Influence culture throughout their organizations
  - Ensure staff knows a credible threat exists
  - Ensure staff knows nuclear security is important
  - Ensure appropriate standards for behaviour are set
  - Set communication standards
  - Set training and professional development norms
  - Reinforce good nuclear security culture actions
  - Seek continual improvement
  - Prevent complacency
  - Ensure good practices are used in nuclear security

Role of Employees

Employees should:

- Be accountable for their behaviour
- Be motivated to ensure nuclear security
- Be professional toward their responsibilities
- Comply with rules, regulations, and procedures
- Be vigilant and questioning
- Recognize the importance of information protection
- Have an underlying feeling of the importance of nuclear security

IAEA

Beliefs and Attitudes

- Basis (foundation) of nuclear security culture
- Exist in people's minds
- Beliefs and attitudes:
  - Developed through experience (shared)
  - Developed over time (individual)
  - Affect individual behaviour
  - Ultimately affect nuclear security effectiveness
- Important for security personnel and also others in the organization

Principles

- Instilled by managers into the organization
- Seen as guiding decisions of management
- Sometimes thought of as “what we say we are going to do”
- Fit into visible category if they are used to guide decisions and behaviour
- Principles for guiding decisions and behaviours are:
  - Commitment and responsibility
  - Leadership
  - Motivation
  - Learning and improvement
  - Professionalism and competence

Principles

- a) Commitment and Responsibility
  - Everyone takes personal responsibility
  - Responsibility for more than just job
  - Responsibility for how security system works as a whole
- b) Leadership
  - Expectations of leaders are great influences on performance
  - Leaders demonstrate their commitment to security
- c) Motivation
  - Encouragement and reinforcement from leaders, peers and subordinates
  - Internalisation of beliefs and values
  - Often set by management

Principles

- d) Learning and Improvement
  - Continual self-assessment
  - Understanding why mistakes occur
  - Application of best practices
- e) Professionalism and Competence
  - Requires that security personnel:
    - Qualified
    - Appropriately skilled
    - Have necessary knowledge (trained)
  - Able to respond to contingencies
  - Correct actions come naturally

IAEA

Management Systems

- Staff performance affected by mana systems
  - Standards for quality of :work
  - Training
  - Documented procedures
  - Information systems, etc.
- Well-developed management system is essential feature of effective nuclear security
- Reflects the nuclear security culture

IAEA

Management system Indicators

- Visible security policy
- Clear roles and responsibilities
- Performance measurement
- Work environment
- Training and qualifications
- Work management
- Information security
- Operations and maintenance
- Determination of staff worthiness
- Quality assurance
- Change management
- Feedback process
- Contingency plans and drills
- Self-assessment
- Interface with regulator

IAEA

Importance of Behaviour

- Behaviour is observable reflection of nuclear security culture
- People learn and imitate prevailing behaviour patterns around them
- Once established, patterns difficult to change
- Behaviour of leadership and all employees includes:
  - Vigilance
  - :Questioning attitude
  - Executing work accurately
  - Adhering to high standards

IAEA

Leadership Behaviour: a) Expectations

- Leaders establish performance expectations
- Low expectations result in low performance

❖ Security culture indicators
  - Specific expectations on nuclear security explicitly communicated by leadership
  - Leading by example
  - Recognize degraded conditions and effect corrections
  - Personally inspect performance (walking, looking, listening)
  - Demonstrate sense of urgency for corrections
  - Ensure resources are available for effective nuclear security

b) Use of Authority

- Authority should be clear and documented for all

❖ Security culture indicators

- Designated managers recognize and take charge when there are changes to vulnerability, security or threat
- Managers are approachable, encourage communication and encourage reporting concern or suspicions
- Leaders do not circumvent security by their authority

IAEA

c) Decision-Making

- Formal and inclusive decision-making process
- Demonstrates significance of security decisions
- Improves quality of decision

❖ Security culture indicators
  - Leaders make decisions when needed
  - Explain decisions when possible
  - Solicit dissenting views to strengthen decision
  - Do not shorten or bypass decision-making process
  - Decisions made by those qualified and authorized

d) Management Oversight

- Nuclear security culture is influenced by supervisory skills
- Absentee managers cannot affect good behaviour

❖ Security culture indicators
  - Managers spend time observing, correcting and reinforcing staff at working locations
  - Corrective feedback is used to reinforce desired behaviour

IAEA

e) Involvement of Staff

- Staff must be able to contribute insights and ideas
- Formal mechanisms in place to allow this to happen

❖ Security culture indicators
  - Where practical, leaders should involve staff in decision-making process
  - Encourage staff members to make suggestions

IAEA

f) Effective Communications

- Encourage and maintain flow of information
- Flow should be throughout the organization

❖ Security culture indicators:
  - Leaders ensure communication is valued and not blocked
  - Explain context for issues and decisions
  - Visit staff at work locations and talk
  - Welcome staff input, take action or explain why no action was taken

g) Improving Performance

- Avoid complacency
- Strive to continuously improve nuclear security performance
- Leaders should show by personal example their expectation to look for ways to learn and improve

❖ Security culture indicators
  - Leaders encourage all levels to report problems and make suggestions
  - Causes of adverse trends identified and corrected
  - Analysis of events involves potential consequences
  - Focus on improvement of a problem and not blame
  - Process exists for everyone to report nuclear security concerns

h) Motivation

- Satisfactory behaviour depends on motivation and attitudes
- Both individual and group motivations are important

❖ Security culture indicators

- Managers encourage and reward commendable behaviour
- Reward system recognizes contributions to nuclear security
- Staff are aware of a system of rewards and sanctions
- Annual performance appraisals include nuclear security issues
- Application of disciplinary measures are tempered to encourage reporting of infractions

IAEA

Employee Behaviour: a) Professional Conduct

- Includes high standards of honesty and integrity

❖ Security culture indicators

  - All employees are familiar with organization's professional code of conduct and adhere to it
  - Take professional pride in their work
  - Help each other and interact with professional courtesy and respect

IAEA

b) Personal Accountability

- All workers know their specific assigned tasks:
  - What to do
  - When to do it
  - Results expected
- Either do tasks correctly or report inability to supervisor

❖ Security culture indicators
  - Staff understand how their tasks support nuclear security
  - Commitments are met or inability reported
  - Behaviour that reinforces security culture reinforced by peers
  - Staff takes responsibilities to resolve issues

c) Adherence to Procedures

- Procedures represent cumulative knowledge and experience
- It is important to follow procedures
- Procedures should be:
  - Clear
  - Up-to-date
  - Readily available
  - User-friendly

❖ Security culture indicators
  - All staff adhere to procedures, including information controls

IAEA

d) Teamwork and Cooperation

- Teamwork is essential to good nuclear security culture
- Works best where relationships are positive and professional

❖ Security culture indicators
  - Teams recognized for contribution to nuclear security
  - Staff interact with openness and trust and support each other
  - Problems solved by multilevel and multidisciplinary teams
  - Teamwork encouraged at all levels and across boundaries

IAEA

e) Vigilance

- Vigilance and observational skills are important
- Prompt identification of vulnerabilities leads to proactive corrective actions

❖ Security culture indicators

- Staff notice and question unusual signs and occurrences
- Staff are attentive to detail
- Staff seek guidance when unsure of security significance of events or occurrences

IAEA

Conclusion

Results: More Effective Nuclear Security

- **Greater assurance that the security system will do the following when personnel do their job:**
  - **Deter**
  - **Detect**
  - **Delay**
  - **Respond**
  - **Mitigate**

IAEA