INMM – Fundamentals of Physical Protection Workshop

Alan Evans, Adam Williams – Sandia National Laboratories
Dr. Adam Williams (Sandia)
- Adam is a Principal R&D System Engineer at Sandia, where he is a PI and SME on research projects for evaluating vulnerabilities in cyber-physical nuclear systems, managing complex risk in the nuclear fuel cycle, and exploring alternatives for the future of the U.S. Cooperative Threat Reduction program

Mr. Alan Evans (Sandia)
- Alan is a Senior R&D nuclear engineer in the International Nuclear Security Engineering (INSE) department at Sandia, where he co-leads the NNSA’s Office of International Nuclear Security (NA-211) Physical Protection Functional Team, developing physical security strategies for advanced reactors, and an effort to develop a new Nuclear Security Program at the University of New Mexico
Keynote Address

David Avalos – NNSA’s Office of International Nuclear Security (Physical Protection Functional Lead)
• David Avalos is a project/program lead in the Office of International Nuclear Security (INS) in the NNSAs Office of Defense Nuclear Nonproliferation. David is a country lead, managing U.S. nuclear security relations with partner countries, the physical protection functional team lead and has a background in physical protection system implementation.
Workshop Introduction

In this workshop you will be exposed to

• The fundamental principles of physical protection
• The fundamentals of international policies
• Socio-political and economic considerations for physical protection systems
• The history of nuclear security
• Engineering functions of physical protection systems
• Challenges from new and emerging threats and advanced nuclear technologies
• Physical security-by-design
Importance of Nuclear Security

- Secure nuclear material and nuclear facilities globally
- International nuclear security regime exists to ensure the secure and safe operations of peaceful nuclear technologies
- Nuclear security regime consists of fixed site security of nuclear material and security of nuclear material in transport
- Fixed site security is built on physical protection systems
  - Detection
  - Delay
  - Response
Nuclear Security Considerations

- Reduction of cost for physical protection systems
  - Security operation costs are some of the largest for nuclear facilities
  - Reduction of technology cost
  - Reduction of installation cost
  - Reduction of operation and maintenance cost

- Improve performance of physical protection systems
  - Improvement of detection technologies
  - Improvement of assessment capabilities
  - Development of novel delay technologies
  - Develop novel security system approaches against emerging threats
  - Develop novel security systems for advanced nuclear facilities
International Nuclear Security Regime
Roadmap

- Define nuclear security
- Identify international binding instruments relevant to nuclear security
- Discuss the purpose and scope of NSS No. 13 with respect to developing and maintaining a physical protection regime
### Fundamental Nuclear Security Documents (International)

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convention on the Physical Protection of Nuclear Material (CPPNM)</td>
<td>Only legally binding undertaking in the area of physical protection of nuclear material used for peaceful purposes</td>
</tr>
<tr>
<td>2005 Amendment to the Convention on the Physical Protection of Nuclear Material</td>
<td>Extends above protection measures to nuclear facilities/materials in peaceful domestic use, storage, or transport; expands cooperation among States regarding locating/recovering/mitigating missing material</td>
</tr>
<tr>
<td>International Convention for the Suppression of Acts of Nuclear Terrorism</td>
<td>Seeks to criminalize unlawful/intentional possession or use of nuclear materials or nuclear facility sabotage</td>
</tr>
<tr>
<td>Security Council Resolutions 1373 (2001) and 1540 (2004)</td>
<td>1373 – calls all States to become party to all international instruments for nuclear security 1540 - calls all States to become party to the CPPNM (and amendment) and IAEA Code of Conduct</td>
</tr>
<tr>
<td>Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities (INFCIRC/225/Rev.5) [NSS-13]</td>
<td>Internationally accepted document for protection of nuclear material. This document utilizes a graded approach against theft and sabotage of nuclear material.</td>
</tr>
</tbody>
</table>
Increasing outsider and insider threats dictate that we elevate nuclear security to the same level of priority as we do for mission (e.g., production or research) and nuclear safety.

<table>
<thead>
<tr>
<th>Nuclear products, power, research, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nuclear safety and radiation protection</td>
</tr>
<tr>
<td>Nuclear security</td>
</tr>
</tbody>
</table>
Prevention Aspects of Nuclear Security

**Prevention** – Deterring or defeating an adversary’s attempt to commit theft, sabotage, unauthorized access, or illegal transfer

Two complementary prevention strategies:
- Eliminate the material and facilities at risk, thereby eliminating the risk
- Protect material and facilities at risk, thereby reducing the probability of a successful malicious act with the use of stolen material or involving sabotage

Two facets of protection:
- Establishing and maintaining effective inventory, accounting, and controls
- Providing physical protection
Physical Protection Objectives

Protect persons, property, society, and the environment from malicious acts involving nuclear material and other radioactive material (2.1)

- Objectives related to theft (2.1)
  - To protect against unauthorized removal: Protecting against theft and other unlawful taking of nuclear material
  - To locate and recover missing nuclear material: Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material

- Objectives related to sabotage (2.1)
  - To protect against sabotage: Protecting nuclear material and nuclear facilities against sabotage
  - To mitigate or minimize effects of sabotage: Mitigating or minimizing the radiological consequences of sabotage
NSS – Four Tiers of Documents

Fundamentals — NSS No. 20
Objectives and Essentials of a State’s Nuclear Security Regime

Recommendations — NSS No. 13
(application of Fundamentals)
Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities

Implementing Guides —
(application of Recommendations, implementation of NSS No. 13)
NSS No. 25G Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities
NSS No. 7 Nuclear Security Culture
NST023 Physical Protection of Nuclear Materials

Technical guidance, reference manuals, training material
NSS No. 17 Computer Security at Nuclear Facilities
NST033 Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility During Storage, Use and Movement
History of NSS No.13

• Information Circular (INFCIRC/225) has been the de facto international standard for the physical protection of nuclear material for decades
  • Since 2011, it has been referred to as NSS No.13

• Originally prepared by a panel of experts convened by the IAEA director general in 1972

• First published in the INFCIRC series in 1975

• Subsequently revised by member-state experts
  ◦ 1977 (Revision 1)
  ◦ 1989 (Rev.2)
  ◦ 1993 (Rev.3)
  ◦ 1999 (Rev.4)
  ◦ 2011 (Rev.5) — Established as NSS No.13
NSS No.13 Objectives for Physical Protection Regimes

To protect against unauthorized removal

- Protecting against theft and other unlawful taking of nuclear material

To locate and recover missing nuclear material

- Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material

To protect against sabotage

- Protecting nuclear material and nuclear facilities against sabotage

To mitigate or minimize the effects of sabotage

- Mitigating or minimizing the radiological consequences of sabotage
Roles & Responsibilities

Roles and responsibilities

◦ For each entity

◦ Joint responsibilities

  ◦ Sustainment
    ◦ Nuclear security culture
    ◦ Quality assurance
    ◦ Confidentiality
    ◦ Sustainability program

◦ Planning and Preparedness
Roles & Responsibilities

1. State/Competent Authority Responsibilities
   - Physical Protection Regime (aka, “Nuclear Security”)

2. License Holder Responsibilities
   - Physical Protection Measures

3. People, Society, Environment
International Best Practices

Achieve objectives through (2.2 & 2.3)

- Prevention of a malicious act by means of *deterrence* and by *protection* of sensitive information

- Management of an attempted malicious act or a malicious act by an integrated system of *detection*, *delay*, and *response*

- *Mitigation* of the consequences of a malicious act

- Addressed in an *integrated* and *coordinated* manner
## International Best Practices: What?

### IAEA Nuclear Material Categorization

<table>
<thead>
<tr>
<th>Material</th>
<th>Form</th>
<th>Category I</th>
<th>Category II</th>
<th>Category IIIc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Plutonium</td>
<td>Unirradiated&lt;sup&gt;ₚ&lt;/sup&gt;</td>
<td>2 kg or more</td>
<td>Less than 2 kg but more than 500 g</td>
<td>500 g or less but more than 15 g</td>
</tr>
<tr>
<td>2. Uranium-235</td>
<td>Unirradiated&lt;sup&gt;ₚ&lt;/sup&gt;</td>
<td>5 kg or more</td>
<td>Less than 5 kg but more than 1 kg</td>
<td>1 kg or less but more than 15 g</td>
</tr>
<tr>
<td></td>
<td>- Uranium enriched to 20% ²³⁵U or more</td>
<td></td>
<td>10 kg or more</td>
<td>Less than 10 kg but more than 1 kg</td>
</tr>
<tr>
<td></td>
<td>- Uranium enriched to 10% ²³⁵U but less than 20% ²³⁵U</td>
<td></td>
<td></td>
<td>10 kg or more</td>
</tr>
<tr>
<td></td>
<td>- Uranium enriched above natural but less than 10% ²³⁵U</td>
<td></td>
<td></td>
<td>10 kg or more</td>
</tr>
<tr>
<td>3. Uranium-233</td>
<td>Unirradiated&lt;sup&gt;ₚ&lt;/sup&gt;</td>
<td>2 kg or more</td>
<td>Less than 2 kg but more than 500 g</td>
<td>500 g or less but more than 15 g</td>
</tr>
<tr>
<td>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 transportation taking all relevant factors into account.)</td>
<td></td>
<td>Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)&lt;sup&gt;d/e&lt;/sup&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes:

- This table is not to be used or interpreted independently of the text of the entire publication.
- All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
- Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded.
- Quantities not falling in Category III and natural uranium: depleted uranium and thorium should be protected at least in accordance with prudent management practice.
- 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.
- Other fuel which by virtue of its original fissile 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/h (100 rad/h) at one meter unshielded.

### IAEA Nuclear Material Categorization
International Best Practices: What?

- Identify vital areas and protect as specified in NSS No. 13
- Graded protection requirements based on level of potential radiological consequences
- Prudent management practices to secure and control access to assets and safety-related equipment

Radiological Consequences
The Threat Is Real

Key nuclear security issues

Rising terrorism worldwide

Domestic issues that could lead to nuclear terrorism:

◦ Extremism
◦ Separatist challenges
◦ Economic motives to steal and sell nuclear material and information
◦ Criminal activities
◦ Unforeseen economic downturns or sociopolitical changes
Socio-Political Considerations
Roadmap

Stakeholders for Nuclear Security
  ◦ International
  ◦ National/State
  ◦ Local

Human Dimensions of Nuclear Security
  ◦ Challenges
  ◦ Threats
  ◦ Opportunities

Threats for Nuclear Security
  ◦ Definitions
  ◦ Assessment
  ◦ Challenges
Stakeholders for Nuclear Security

Security for nuclear facilities and materials is the *right* and *responsibility* of every sovereign state.

State government establishes laws for the nuclear security (often called “physical protection regime”)

Competent authority(ies) establishes regulations and is responsible for oversight of physical protection regime
- *Prescriptive* and *performance-based* requirements

Facility operators implement physical protection systems aligned with the regime and state requirements.

*Includes operators, shippers, and...*
Stakeholders—International

Roles
◦ Encourage effective security capacity
◦ Support coordination/collaboration efforts

Responsibilities
◦ Establish international best practices
◦ Provide improvement opportunities

Examples
◦ International Atomic Energy Agency (IAEA)
◦ World Institute for Nuclear Security (WINS)
◦ Institute for Nuclear Materials Management (INMM)

*Includes operators, shippers, and...

State
Establishes
Competent Authority
Implements legislation and regulations
License Holders*
Implements Physical Protection
Stakeholders—National/State

Roles
◦ Support/sustain nuclear security capacity
◦ Legislate/oversee protection of nuclear facilities/materials

Responsibilities
◦ Identify/assign competent security authority
◦ Establish/monitor performance requirements

Examples
◦ Regulator (e.g., US Nuclear Regulatory Commission)
◦ CSA (e.g., US National Nuclear Security Administration)
◦ R&D (e.g., US National Laboratories)

*Includes operators, shippers, and
Other stakeholders *can* include:

- Military/national police force
- Intelligence community
- Transportation entities
- Industry groups (e.g., PWROG, BWROG)
- Professional societies (e.g., INMM)
- Academia (e.g., courses, certificates, research)

*Includes operators, shippers, and...*
Stakeholders—Local

Roles
- Translate legislation & regulations into system design
- “Pointy end of the spear” for protecting nuclear materials

Responsibilities
- Designing/implementing security systems
- Aligning security with normal facility operations

Examples
- Nuclear power plants (e.g., Watts Bar NPP in TN)
- Research reactors (e.g., AGN reactor at UNM)
- NFC facilities (e.g., Framatome in WA)
Stakeholders

Multi-level stakeholder responsibilities → basic assumptions for successful physical protection systems

- State-level  →  Requirements exist
- Competent Security Authority-Level  →  Solutions to requirements are implemented
- License Holder-Level  →  The behavior(s) of implemented solutions is observed/analyzed
Human Dimension + Challenges

All nuclear-security risks have a *human* dimension.

Personnel play a positive role …
- Preventing, detecting, and responding to nuclear security events
- Regulating, inspecting, and evaluating nuclear security in practice

Personnel can also play a negative role
- Facilitate nuclear security incidents through …
  - Negligence
  - Lack of awareness/knowledge
  - Accidental or unintentional acts
  - Malicious acts – the “*insider threat*”
Human Dimension + Challenges

All nuclear-security risks have a *human* dimension.

Personnel play a positive role …
- Preventing, detecting, and responding to nuclear security events
- Regulating, inspecting, and evaluating nuclear security in practice

Personnel can also play a negative role
- facilitate nuclear security incidents through …
  - Negligence
  - Lack of awareness/knowledge
  - Accidental or unintentional acts
  - Malicious acts – the “*insider threat*”

Insiders have (and can exploit!):

- **Access**
- **Authority**
Human Dimension + Threats

**Koeberg Nuclear Power Station (South Africa)**

- **Who:** Rodney Wilkinson (Olympic level athlete)
- **What:** Employed by ANC to sabotage the plant
- **Result:** 4 explosions in 1982, significant damage to reactor

**Luch Scientific Production Association (Russia)**

- **Who:** Leonid Smirnov (chemical engineer)
- **What:** Smuggled total of 1.5 kg of HEU over 5 months
- **Result:** No buyer, testing the market; eventually arrested on other charges

**Doel Nuclear Power Station-Unit 4 (Belgium)**

- **Who:** Unknown
- **What:** “Voluntary manual operation” to drain turbine lubricant → apparent sabotage
- **Result:** Plant shut down, severe doubt about security
All nuclear-security risks have a human dimension.

Personnel play a positive role …
- Preventing, detecting, and responding to nuclear security events
- Regulating, inspecting, and evaluating nuclear security in practice

Humans can creatively counter adversaries:
- Adapt
- Assess
- Anticipate
Some proposed (and widely accepted) definitions (per the IAEA Nuclear Security Series No. 13)

- **Threat**: a person or a group of persons with motivation, intention and capability to commit a malicious act

- **Threat assessment**: an evaluation of threats – based on available intelligence, law enforcement, and open source information – that describes the motivations, intentions, and capabilities of these threats
One popular approach to translating threat assessments into something more engineering design-friendly is the design basis threat (DBT). The DBT defines attributes and characteristics of adversaries deemed to have intent and capabilities to commit a malicious act. It heavily borrows from the design basis accident and probabilistic tradition of nuclear safety. The design basis threat is an ERDA-7 proposal for both safety and security.
DBT → Development Process

DBT is *one solution* for security as “high consequence, low probability”
- How much security is enough? How do we know?

DBT provides a stable, defensible *design criteria* to support
- Efficient allocation of resources
- Performance baseline for evaluations

Establishes *threat-based* criteria for design, evaluation, accountability

Foundation for *agreement between* State & Operator regarding:
- Threat capabilities that are being protected against
- Who has primary responsibility for protection against given threats
- Level of risk accepted
Threats—Challenges

Complex & complicated world of threat identification
- Incomplete, imperfect data input streams
- Trustworthiness of sources
- Timeliness/accuracy of sharing information

Pace of adaptability in “information age”
- Significant increase in tactical capabilities—global, domestic
- Increased knowledge to support successful breaches
- Technological revolutions
  - UAS
  - Cyber – globally, domestically
  - Others…

Facility-level operational realities
- Resource-constrained environments
- “Boy who cried wolf” phenomenon
- Multi-stakeholder problems (e.g., competing interests)

Socio-cultural barriers to adoption/appreciation
- “We’re not targets, what’s the big deal”
- “It could never to happen to us”
- Social engineering of personnel (Abraham & Chengalur-Smith 2010)
Roadmap

Stakeholders for Nuclear Security
- International \(\rightarrow\) Supports coordination/collaboration on best practices (e.g., IAEA)
- National/State \(\rightarrow\) Establishes/encourages security performance requirements (e.g., USNRC)
- Local \(\rightarrow\) Designs/implements security systems (e.g., NPPs)

Human Dimensions of Nuclear Security
- Challenges \(\rightarrow\) All security risks have a human dimension
- Threats \(\rightarrow\) Not only external adversaries, must also consider insider threats
- Opportunities \(\rightarrow\) Most security solutions have a human dimension

Threats for Nuclear Security
- Definitions \(\rightarrow\) Threats = potential capabilities vs. TA = capabilities against a facility
- Assessment \(\rightarrow\) DBT is one solution, threat-based design criteria
- Challenges \(\rightarrow\) Threat ID, pace of adaptability, operational realities, socio-cultural barriers
Economic and Budget Considerations
Economic and Budget Considerations

Class Discussion

Why is it important to consider security and its impact on the budget at a nuclear facility?
Roadmap

• Initial Technology Cost
  • Technology Design
  • Technology Purchase

• Initial Installation Cost
  • Tools
  • Labor

• Performance Testing
  • Labor

• Operations Cost
  • Personnel
  • Power

• Maintenance
  • Tools
  • Replacement
Economic and Budget Considerations

Security system designers must understand the cost of implementing a security system

- Initial technology cost
- Initial installation cost
- Performance testing costs
- Operations costs
- Maintenance cost
Initial Technology Cost

Security systems require the purchase of technologies and material

- **Intrusion detection technologies**
  - Sensors, cameras, thermal cameras, RADAR, etc.

- **Barriers**
  - Vehicle barriers, security doors, fences, vault doors, etc.

- **Access control technologies**
  - Badge readers, biometrics, facial recognition, badge and PIN readers

- **Communication networks**
  - Fiberoptic cable, phone lines, radio networks, etc.

https://www.tonex.com/training-courses/introduction-systems-engineering-
Initial Installation Cost

Installation cost is a cost that must be considered when understanding the overall cost of a security system. Installation requires intensive man hours and equipment to install security technologies:

- Trenching equipment
- Necessary tools
- People required to install equipment

https://www.tonex.com/training-courses/introduction-systems-engineering-lifecycle-processes/
Performance testing is another cost that is often not considered in the initial design of a facility.

Tests often needed to be conducted regularly:
- Varying on level of importance of the technology
- Varying on the design lifecycle of the technology
- Varying on the location of the technology
Operations Cost

Operations cost includes
- Guards
- Responders
- Alarm station operators

Operations costs also include
- Power/electricity costs
- Other utilities

https://www.tonex.com/training-courses/introduction-systems-engineering-lifecycle-processes/
Maintenance is often an expense that is not considered in the initial design. Technologies that require less maintenance may have an increased purchase cost.

Maintenance costs incorporate:
- Man-hours needed to conduct maintenance
- Replacement technology cost
- Increased response or guard presence as a compensatory measure

https://www.tanex.com/training-courses/introduction-systems-engineering-lifecycle-processes/
Designing Security Systems

Security system designers must consider the various cost impacts of systems

Man-hour intensive systems may cost less than technology intensive systems
  ◦ When labor costs are lower

Technology intensive systems may cost less than man-hour intensive systems
  ◦ When labor costs are higher
Additional Considerations

Compensatory Measures
  ◦ Man-hour intensive

Personnel
  ◦ Staffing, overtime, high turnover rates, etc.

Training
  ◦ Initial and ongoing training
    ◦ Schedule, time, resources

Equipment
  ◦ Repair, replacement, obsolescence

Force-on-Force
  ◦ Scheduling, time, equipment, resources

Routine Site Support
  ◦ Searches, escorts, material transfers, planned compensatory measures
Summary

• Initial Technology Cost
  • Technology Design
  • Technology Purchase

• Initial Installation Cost
  • Tools
  • Labor

• Performance Testing
  • Labor

• Operations Cost
  • Personnel
  • Power

• Maintenance
  • Tools
  • Replacement
Physical Security System Trade-Offs
Roadmap

Physical Protection System Design Considerations
- Objectives
- Functions

Physical Protection System Design *External* Tradeoffs
- Cost vs. Performance
- Best practice vs. Regulation

Physical Protection System Design *Internal* Tradeoffs
- System behaviors vs. component capability
- Technology vs. People
PPS Design Considerations—Objectives

Safety vs. Security

Similarities
○ Goal = prevent radiological release/unauthorized access
○ Address a series/interconnected events
○ Attempts to describe uncertainty in desired operations

Differences
○ Random events vs. Targeted actions
○ Acts of nature vs. Actions of people
○ Accidents vs. Intentional acts
PPS Design Considerations—Objectives

Prevent theft of nuclear materials

- Recover/recapture stolen nuclear materials

Prevent sabotage of nuclear materials/facilities

- Minimize consequence of any sabotage event

***NOTE: These must be achieved in alignment with normal facility operations!***
PPS Design Considerations—Functions

Detection: discovery of an adversary action

Delay: slowing of an adversary action

Response: actions by the response force against adversary actions

Protect = f(detect, delay, respond)
PPS Design Considerations

- Physical Protection Measures
- Physical Protection Systems
- Physical Protection Regime(s)

Objectives interpreted → Functions identified → Functions implemented

Objectives evaluated → System behaviors → Component capability
PPS Design—External Tradeoffs

**Costs** for physical protection systems
- Accrued cross system lifecycle
  - Design → installation → operations → maintenance
- Non-insignificant portion of regular nuclear facility operating budgets

**Performance** for physical protection systems
- Major component of overall risk reduction
  - Key element of public/social acceptance
- Assessed continually for the entire PPS
PPS Design—External Tradeoffs

Costs
- Production pressures
- Severe budget constraints

Performance
- Constrained capabilities
- Lower quality components

Costs
- Larger security budgets
- Limited budget constraints

Performance
- Enhanced capabilities
- Higher quality components
PPS Design—External Tradeoffs

**Best practices** for physical protection systems
- Consensus-based approach to establishing standard for “good enough”
- Voluntary agreements aimed at consistency/effectiveness
- Little (if any) punitive measures for insufficient/ineffective implementation

**Regulations** for physical protection systems
- Legislation-based approach to establishing standard for “good enough”
- Required set of agreements defining consistency/effectiveness
- Legal/financial punitive measures for insufficient/ineffective implementation
Best Practices

- Different interpretations
- Contradictions to regulations

Regulations

- Best practices as additional efforts
- Limited resources stretched farther

Best Practices

- More effective regulation implementation
- Stronger PPS with both

Regulations

- Can drive improvements in quality of best practice
- Stronger PPS with both
PPS Design—External Tradeoffs

Objectives interpreted

Functions identified

Functions implemented

Best practices

Physical Protection Regime(s)

System behaviors

Costs

Physical Protection Systems

Performance

Physical Protection Measures

Component capability

Objectives evaluated
**System behavior(s)** for physical protection systems
- Observed performance of the PPS over time
- Designed at a point in time $\rightarrow$ operations $\rightarrow$ maintenance
- Must include impacts of *interactions* between components

**Component capability** for physical protection systems
- Reliability, efficiency, & effectiveness of individual components
- Can select component to optimize a particular security function
PPS Design—External Tradeoffs

System behavior
- Sub-optimal system performance

Component capability
- Optimized, uncoordinated components

System behavior
- Optimal, effective system performance

Component capability
- Non-optimized, coordinated components
PPS Design—External Tradeoffs

**Technologies** for physical protection systems
- Better for aggregating lots of data & signal discrimination
- Large variety & highly customizable
- High reliability over **longer** timeframes

**People** for physical protection systems
- Better for analyzing data & recognizing patterns
- More flexible, mobile deployment
- High reliability over **shorter** timeframes
PPS Design—External Tradeoffs

Technologies
- High reliability over longer timeframes
- Better detection
- Better data collection

People
- High reliability over shorter timeframes
- Better assessment
- Better data analysis

Technologies
- Data aggregation to aid decision making
- Support anomalous pattern detection

People
- Incorporating more system data into decisions
- Execute better pattern detection
PPS Design—Internal Tradeoffs

Objectives interpreted

Functions identified

Functions implemented

Physical Protection Regime(s)

Physical Protection Systems

Physical Protection Measures

Technologies

People

System behaviors

Component capability

Objectives evaluated
Roadmap

Physical Protection System Design Considerations
- Objectives \(\rightarrow\) prevent theft; recover/recapture; prevent sabotage; min consequences
- Functions \(\rightarrow\) \textit{PPS performance} = \textit{f(detection, delay, response)}

Physical Protection System Design \textit{External Tradeoffs}
- Cost vs. Performance \(\rightarrow\) traditional resource constraint issues
- Best practice vs. Regulation \(\rightarrow\) flexibility & consensus vs. rigidity & enforcement

Physical Protection System Design \textit{Internal Tradeoffs}
- System behaviors vs. component capability \(\rightarrow\) component interactions matter
- Technology vs. People \(\rightarrow\) need to balance/leverage relative strengths of each
History of Nuclear Security
Introduction
U.S. Nuclear Security during the Manhattan Project

Los Alamos
Gate 1942

US Army Military Police Detachment
Military or Civilian Control Of Atomic Energy?

The controversy "should atomic energy be under military or civilian control?" has been brought to a showdown in the Senate Special Committee on Atomic Energy.

In the extreme militaristic side, there is Senator Eugene D. Millican of Colorado who believes that even General Groves favors too much civilian influence. But in justice to General Groves, his scheme of an Atomic Energy Commission containing four military men and nine members with an active officer as administrator can be relied upon to bring about complete military control.

The argument in favor of having research and development of atomic energy in the hands of the military goes as follows: "The atomic bomb is the most powerful weapon in existence. The applications of atomic energy to purposes of military importance can be postponed without endangering our national security. With the world political situation as it is, we must give first priority to the military problem, and this can best be achieved by leaving the control of atomic energy in the hands of the military."

President Truman signs the Atomic Energy Act into Law
Terrorism
THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. O. S. Buckley.

Very sincerely yours,

[Signature]

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.
Systems Engineering and Nuclear Security

Design and Evaluation Process Outline (DEPO)

- **Define System Objectives**
  - Asset Identification
  - Assets and Operations Characterization
  - Threat Assessment

- **Characterize System**
  - Physical Protection System Functions
    - Detection
    - Delay
    - Response

- **Evaluate System**
  - Systems Analyses
  - System Evaluations
  - Modeling and Simulation
  - Performance Testing

- **Effective**
  - Not Effective

- **Redesign System and/or Modify System Objectives**
Conclusion

The world is changing
- New and Emerging Threats
- New Technologies

The core systems engineering principles and concepts introduced 50 years ago are still valid today

Systems engineering can provide a framework for incorporating new technologies and revolutionize the age old nuclear security concepts of Guns, Gates, and Guards