INMM Physical Protection Workshop Series: Security-by-Design

March 15th-March 17th, 2022
Workshop Introduction

Dr. Adam Williams (Sandia)
- 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 alternative futures of the U.S. Cooperative Threat Reduction program

Mr. Alan Evans (Sandia)
- Senior R&D nuclear engineer at Sandia, where he co-leads the NNSA's Office of International Nuclear Security (NA-211) Physical Protection Functional Team, PI for reduced cost PPS for the DOE-NE ARS Program, and co-lead of the UNM Nuclear Security Program

Mr. Joe Rivers (Rivers Security Services)
- Nuclear security consultant with over 35 years of experience in nuclear safeguards and security, with current projects related to UAS, advanced reactors, research reactors, decommissioning, reactor sabotage, security for a new HALEU fuel fabrication facility
Keynote Address

Joe Sandoval
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 Ervin D. Milhous 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 among its nine members with an active officer as administrator can be relied upon to bring about complete military control.

The argument in favor of keeping 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 application of atomic energy to war purposes will permit the utilization of forces which can be used without endangering our national economy. 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.

Secret regulations, which military mentality is likely to force upon fundamental scientific research, will cause a paralyzing of scientific progress. This paralysis will spread from governmental atomic bomb laboratories to all laboratories working in the nuclear field. The necessity may arise for secrecy laws to become a dead letter with other regulations leaving the majority of scientists in ignorance of both facts of their science. With nuclear physics as an opening wedge, the same diminution may permit the fields of bacteriology, medicine, and other sciences all of which may be used in the next total war.

President Truman signs the Atomic Energy Act into Law
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,

Henry A. Wallace

Mr. Leroy A. Wilson,  
President,  
American Telephone and Telegraph Company,  
135 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

- Redesign System and/or Modify System Objectives

Effective vs. Not Effective
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
International Nuclear Security Regime
Outline

• 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
<table>
<thead>
<tr>
<th><strong>Fundamental Nuclear Security Documents (International)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convention on the Physical Protection of Nuclear Material (CPPNM)</strong></td>
</tr>
<tr>
<td><strong>2005 Amendment to the Convention on the Physical Protection of Nuclear Material</strong></td>
</tr>
<tr>
<td><strong>International Convention for the Suppression of Acts of Nuclear Terrorism</strong></td>
</tr>
</tbody>
</table>
| **Security Council Resolutions 1373 (2001) and 1540 (2004)** | 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. |
| **Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities (INFCIRC/225/Rev.5) [NSS-13]** | **Internationally accepted** document for protection of nuclear material. This document utilizes a graded approach against theft and sabotage of nuclear material. |
Nuclear Security as a Priority

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.
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

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

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
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
  o 1977 (Revision 1)
  o 1989 (Rev.2)
  o 1993 (Rev.3)
  o 1999 (Rev.4)
  o 2011 (Rev.5) — Established as NSS No.13
 NSS No.13 Objectives for Physical Protection Regimes

To protect against unauthorized removal
  o Protecting against theft and other unlawful taking of nuclear material

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

To protect against sabotage
  o Protecting nuclear material and nuclear facilities against sabotage

To mitigate or minimize the effects of sabotage
  o Mitigating or minimizing the radiological consequences of sabotage
Roles and responsibilities

- For each entity
- Joint responsibilities
  - Sustainment
    - Nuclear security culture
    - Quality assurance
    - Confidentiality
    - Sustainability program
  - Planning and Preparedness
Roles & Responsibilities

- People
- Society
- Environment

Physical Protection Regime (aka, “Nuclear Security”)

Physical Protection Systems

Physical Protection Measures

License Holder Responsibilities

State/Competent Authority Responsibilities
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: From the CPPNM

<table>
<thead>
<tr>
<th>Material</th>
<th>Form</th>
<th>Category I</th>
<th>Category II</th>
<th>Category IIc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Plutonium</td>
<td>Unirradiated(^b)</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(^b)</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% (^{235}\text{U}) or more</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Uranium enriched to 10% (^{235}\text{U}) but less than 20% (^{235}\text{U})</td>
<td>10 kg or more</td>
<td>Less than 10 kg but more than 1 kg</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Uranium enriched above natural but less than 10% (^{235}\text{U})</td>
<td>10 kg or more</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Uranium-233</td>
<td>Unirradiated(^b)</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</td>
<td>(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>Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)(^d/e)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This table is not to be used or interpreted independently of the text of the entire publication.

\(^a\) 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/h (100 rad/h) at 1 m unshielded.

\(^c\) 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 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.
International Best Practices: Radiological Consequences

- Identify vital areas
- High Radiological Consequence (HRC) Threshold
- Graded protection requirements based on level of potential radiological consequences
- Unacceptable Radiological Consequence (URC) Threshold
- Prudent management practices to secure and control access to assets and safety-related equipment

Potential Sabotage 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
Traditional Security Design Strategies: A Depo Perspective
Process for Developing the PPS Design

**Define PPS Requirements**
- Facility Characterization & Target Identification
- Threat Definition
- Risk Management & Regulatory Requirements

**Design PPS**

**Physical Protection System**
- Detection
  - Intrusion Detection
  - Access Control
  - Prohibited Items Detection
  - Alarm Assessment
  - Alarm Comm. & Display
  - Insider Design
- Delay
  - Access Delay
- Response
  - Response
  - Nuclear Program Plans

**Evaluate PPS**
- Adversary Sequence Diagrams
- Multipath Interruption Analysis
- Neutralization Analysis
- Scenario Analysis
- Tabletop Analysis
- Insider Analysis

**Final PPS Design**

**Redesign PPS**

**Performance Testing**
Basic PPS Functions

**Detection**
- Intrusion Sensing
- Access Control
- Prohibited Item Detection
- Alarm Assessment
- Alarm Communication and Display (AC&D)

**Delay**
- Passive Barriers
- Active Barriers

**Response**
- Guards
- Response Force

Technology – Alarm Station Operators – Guards
Detection Process

Performance measures

$P_D$ is the likelihood that an intruder will be detected under a well-defined set of conditions

$$P_D = P_S \times P_A$$

- Probability of (alarm) sensing ($P_S$)
- Probability of correct assessment ($P_A$)

```text
<table>
<thead>
<tr>
<th>Sensor Activated</th>
<th>Alarm Signal Initiated</th>
<th>Alarm Reported</th>
<th>Alarm Assessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Alarm Station Operators</td>
<td>Guards</td>
<td></td>
</tr>
</tbody>
</table>
```
Delay Process

Performance measures

Time to penetrate or bypass barriers

Time to travel across areas

Provide Obstacles to Increase Adversary Task Time

Passive Barriers

Active Barriers
Response Process

Performance measures

Probability of communication to response force

Communication time

Probability of deployment to adversary location

Deployment time

Response force effectiveness

Communicate to Response Force → Deploy Response Force → Interrupt Adversary → Neutralize Adversary
Challenges Using Traditional Security Design Strategies
Outline

- Economics
- Emerging Threats and Technologies
- Changing Regulatory Landscapes
- Evolving Threats
Economics

- Security is a large cost for the current fleet of nuclear power plants (NPPs)
  - Operation & Maintenance cost to protect nuclear power plants account for 7% of power generation

- Physical security costs are made of
  - Labor costs
  - Service costs
  - Material costs

- Labor costs for security at nuclear power plants have increased since 2008
  - Account for 60% of the total physical security budget

https://www.tonex.com/training-courses/introduction-systems-engineering-lifecycle-processes/
How can we address economics in security?

• Manpower-intensive vs. technology-intensive systems
  • Manpower intensive systems are more cost effective when labor costs are low
  • Technology-intensive systems are more cost effective when labor costs are high

• Addressing economics in design
  • Incorporate economic analysis in the evaluation of the DEPO methodology
  • Incorporating economic requirements into the design phase of the DEPO methodology
  • Ensuring that economics is included in the design phase of the DEPO methodology

• Designing physical protection systems with decreased infrastructure
  • Reducing operation costs
  • Reducing maintenance costs
  • Reducing sustainability costs
Emerging Threats and Technologies

- Changed in technologies that can be used by adversaries and site security systems
  - Examples
    - Wireless communications
    - Unmanned Aerial Systems
    - Quantum computing

- Emerging technologies and threats may provide tactical advantages to adversaries
  - Example: UAS to bypass security elements

- Emerging technologies may be utilized by the security system to improve performance
  - Example: UAS for detection and assessment
How do we address emerging threats and technologies?

• Consider how emerging threats and technologies can be used within a security system

• Example: UAS for detection and Assessment
  • Advancements allow for thermal imaging and video recording to be implemented in tandem with UAS systems
  • Advancements allow for replacing patrols normally conducted by guards or responders
  • UAS may be used to implement contingency measures when other technologies fail reducing operation costs

• Example: Wireless Communications
  • Ensure cybersecurity measures are in place to prevent vulnerabilities from being exploited
  • Use of wireless communication systems to decrease communication infrastructure costs
Changing Regulatory Landscape

- Regulations may becoming more risk-informed
  - Regulations that allow for the State to determine what risk the State is willing to take on and alleviate an operator from

- Risk-informed regulations may consider
  - Crediting safety systems for security
  - Reducing the threat that an operator must defend against
  - Using radiological consequences to bound security system requirements

- Regulatory landscapes may consider the needs of an operator
  - Costs incurred by operator
  - Need for nuclear energy in energy security strategies
Evolving Threats

• Adversaries continually change and evolve

• Changes in adversary motives
  • Terrorism
  • Capital gain
  • Protests
  • Organized Crime

• Changes in adversary capabilities
  • Access to new technologies
  • Access to new methodologies
  • Access to information
How do we address evolving threats?

Nuclear facilities *may* draw intention from adversaries

This attention *may* become specific threats to a facility that need to be identified

Identified threats *should* be assessed for potential impact of capabilities

These capabilities *may* be described in terms of a model or framework

Protective changes to facility *should* be implemented as mitigations

Such changes *restart* the cycle
Small Modular Reactors and Impacts on Physical Protection System Design
Outline

- Improved Reactor Systems and Designs
- Smaller Footprint Sites
- Reduced Operational Needs
- Need for Reduced Cost Security Systems
Improved Reactor Systems and Designs

• Improved reactor designs that:
  • Potentially decrease reactor refueling
  • Rely more on passive safety systems
  • May have higher fuel burnup

• Decrease in reactor refueling needs
  • May not require fresh fuel storage onsite → Reducing security costs required for fresh fuel storage

• Reliance on passive safety systems
  • May decrease security needs to protect forced safety systems
  • May be able to credit inherent reactor safety for security purposes

• Higher fuel burnup
  • May increase radiological consequences associated to spent fuel
Smaller Footprint Sites

- Smaller footprint sites may
  - Require increased delay measures to allow for an effective response force
  - Require improved detection and extended detection to improve the performance of security systems

- Smaller footprints in a modular design
  - Increase the number of targets needed to protect in a smaller space
  - Require robust designs for effective detection, delay and response
Reduced Operational Needs

- Due to the smaller nature and long core lifetimes
  - Small modular reactors may have decreased operational needs compared to traditional NPPs
  - Small modular reactors may need less security staff and personnel to implement security needs

- Reduced operational needs may allow for the uses of advanced security technologies
  - Active delay → Used to increase adversary task times
  - Automated systems used for security purposes
Reduced Cost Security Systems

• Small modular reactors have expressed interest in reduced cost systems

• Due to the smaller energy output SMRs
  • Must reduce cost of electricity production ($/MWh)
  • Must reduce need for personnel required

• Need for systems that reduce security costs
  • Reduce security infrastructure costs
  • Reduce number of personnel needed for security
  • Reduce security system operational, maintenance, and sustainability costs
Fundamental Principles

- Principle #1: *Intentionality*
- Principle #2: *Minimize (vs. Eliminate) Security Risk*
- Principle #3: *Security is Dynamic & Evolves*
- Principle #4: *Nuclear Security Sustainability Matters*
Principle #1: Intentionality

- Malicious actions → targeted, specific, optimized acts
- Adaptable, dynamic, flexible to increase exploitability
- Fundamentally different to define, describe, forecast
  - Intentional acts do not fit nicely into statistical models
- Approaches: control vs. deter vs. prevent vs. detect vs. delay vs. respond vs. recover
Fundamental Principles

Principle #1: Intentionality

Examples:

- November 2007: Incursion into Pelindaba Nuclear Station
- July 2012: Protestors breaching Y-12 Complex
- Spring/Summer 1992: L. Smirnov stole 1.5 kg of HEU from Luch Plant
Fundamental Principles

Principle #2: *Minimize (vs. Eliminate) Security Risk*

- Intentionality → all vulnerabilities *cannot* be eliminated
  - Can only eliminate security risk by *not* building nuclear facilities

- Security risk is like rushing water, will always find a way

- Parallel to *law of diminishing returns*

- Uncertainty vs. vulnerability vs. susceptibility vs. risk
Fundamental Principles

Principle #2: **Minimize (vs. Eliminate) Security Risk**

Examples:

- 2000s/2010s: NNSA consolidation of Category I nuclear materials
  - Fewer sites with SNM vs. more SNM per site

- “Every dollar spent on security is a dollar not spent on activities that will bring in revenue” [M. Bunn 2010]
  - Financial efficiencies...

- “there is no comprehensive analytical basis for defining the attack strategies an adversary might employ or the probabilities of success associated with them...Using structured thinking processes and techniques to characterize security risk could improve NNSA’s understanding of security vulnerabilities” [C/SWNC 2010]
Fundamental Principles

Principle #3: *Nuclear Security is Dynamic & Evolves*

- A version of the “security dilemma”
- Demonstrated vs. anticipated red/blue capabilities
- Dynamism $\rightarrow$ *increased* uncertainty for security
  - Security included *multi-domain* dynamism
- Proactive vs. reactive strategies/approaches
Fundamental Principles

Principle #3: *Nuclear Security is Dynamic & Evolves*

Examples:

- 9/11 terrorists → shoe bomber → underwear bomber → bombs in printers in the cargo bay → ???
- NNSA: 1980s “law enforcement” → 1990s/2000a professional paramilitary
- UAS:
  - For adversary (2019 attacks on KSA oil fields)?
  - For response force (surveillance and monitoring extended perimeters)?
Principle #4: *Nuclear Security Sustainability Matters*

- Concept of “punctuated equilibrium”
- Absolute need for consistency, vigilance, good security performance
- Long operational lifecycles (per fuel cycle activity)
- Changing security needs across nuclear fuel cycle operations
Fundamental Principles

Principle #4: *Nuclear Security Sustainability Matters*

Examples:

- NNSA & NRC: fixed site vs. transportation security
- Lingering concerns over nuclear waste
  - Security for wet storage vs. dry casks vs. final disposition
- “Guards are quite aware of how precious the objects are that they guard—and how important it is that they be kept safe from an external threat. Yet there is an enormous gap between the abstract importance of their function, and the immediate (and often excruciating) boredom of their job” (Charlton & Hertz 1989)
A Holistic Approach

Requirements

Performance

Implementation
A Holistic Approach

Nuclear Security

Requirements
- Nuclear Facilities and Materials
- Updated Threat

Implementation
- Technology
- Personnel

Performance
- Technology
- Personnel
A Holistic Approach to Physical Protection System Design

- Physical Protection Requirements
- Nuclear Facility and Nuclear Material
- Updated Facility and Material Threat
- Integration of Subsets
- Physical Protection Implementation
- Nuclear Facility and Nuclear Material
- Updated Facility and Material Threat
- Physical Protection Performance
- Nuclear Facility and Nuclear Material
- Updated Facility and Material Threat
Aligning Emergent Properties of Small Modular Reactors
What is an Emergent Behavior?

Emergent behavior is observed performance of a system that cannot be traced back to operations of its individual parts.

- By extension, this suggests such observed performance is partially generated by the *interactions* or *relationships* between individual parts.
Small Modular Reactors as a System

- Emergent behaviors provide a useful frame for understanding or anticipating the operations of Small Modular Reactors, including:
  - Consider the SMR facility as the whole system
  - Consider safety, and security as parts of the system
- Example System Objective: To produce electrical power in a cost-effective manner
  - Relevant security question: how can security-related solution support this objective?
Goals of the Parts

• For SMRs, “cost effective” also includes safety and security concerns:

• **Safety goal:**
  • Develop & deploy systems to protect people and the environment from radiological consequences *caused by accidental events*

• **Security goal:**
  • Develop & deploy systems to protect people and the environment from radiological consequences *caused by malicious actors*

• Components, parts & sub-systems *may* have similar goals, but also have unique aspects
  • The interactions between them despite commonalities, can result in emergent behaviors
Behaviors of the Parts

• Safety $\rightarrow$ control, cool, contain
  • Ensure protection of the reactor and spent fuel caused by an accident or external event
  • Use of natural circulation to ensure reactor safety
  • Use of redundant and advanced components to ensure reactor/spent fuel safety

• Security $\rightarrow$ detect, delay, respond
  • Ensure protection of the reactor and spent fuel caused by malicious adversaries
  • Coordination with armed response force members to ensure reactor protection
  • Use of redundant security technologies to ensure the reactor/spent fuel protection
Emergent Behaviors of Small Modular Reactor Facilities

• Increased system performance has been created by
  • Advances in technology that improve the parts of the system
    • Ex.: New sensors with extended ranges & measurement sensitivities
  • Improved efficiencies within each part of the system
    • Ex.: New sensors with extended ranges & measurement sensitivities that help reduce NAR/FAR
  • Deeper understanding of the interactions & relationships between parts of the system
    • Ex.: New sensors with extended ranges & measurement sensitivities that help reduce NAR/FAR, leading to reduced need for delay at parts of the facility

• Decreased operational needs of the system by
  • Reducing operational complexity within the parts of the system
    • Ex.: Possibility of designing complex (sub)system performance from a few simple, cheap parts
  • Leveraging the beneficial interactions between parts of the system
    • Ex.: Taking “security credit” for core reactor/safety infrastructure design decisions
  • Reducing maintenance and sustainability costs within parts of the system
    • Ex.: Monitoring security as an emergent property = basis for preventive/anticipatory maintenance program
Physical Protection Systems and Emergent Behaviors

• Considering SMR facilities as complex systems $\rightarrow$ security is an emergent behaviors
  • Accounting for interactions & relationships impact the design of physical protection systems

• Physical protection systems in combination with advanced safety systems create a unique feedback loop in designing security systems for SMR facilities
  • Passive/inherent safety $\neq$ passive security; but they are related!

• Impact on physical protection systems (representative examples)
  • Unique PPS designs that protect natural circulation systems
  • Incorporating security into facility infrastructure & procedural design to help reduce overall costs
  • Adaptable PPS design philosophy aligned with increased options for SMR deployment
Functions of a Physical Protection System
Traditional Functions of a Physical Protection System

**Detection**
- Intrusion Sensing
- Access Control
- Prohibited Item Detection
- Alarm Assessment
- Alarm Communication and Display (AC&D)

**Delay**
- Passive Barriers
- Active Barriers

**Response**
- Guards
- Response Force

PPS Functions

Technology – Alarm Station Operators – Guards
Detection Process

Performance measures

\[ P_D = P_S \times P_A \]

- Probability of (alarm) sensing \( (P_S) \)
- Probability of correct assessment \( (P_A) \)
Delay Process

Performance measures

Time to penetrate or bypass barriers

Time to travel across areas

Delay

Provide Obstacles to Increase Adversary Task Time

Passive Barriers

Active Barriers
Response Process

Performance measures

Probability of communication to response force

Communication time

Probability of deployment to adversary location

Deployment time

Response force effectiveness

1. Communicate to Response Force
2. Deploy Response Force
3. Interrupt Adversary
4. Neutralize Adversary
Physical Protection System Strategies

- **Denial**: Used for protecting acts of sabotage against systems, structures, components (SSCs), and nuclear or radioactive material
  - **Denial of Access** → Technology Intensive
    - Denying adversaries access to locations where vital SSCs or material may be located
  - **Denial of Task** → Manpower Intensive
    - Denying adversaries from completing a task at SSCs or material

- **Containment**: Used for protecting nuclear or radioactive material from theft
Integration of PPS Functions

Systems-level PPS design considerations

• Defense in Depth
  • Multiple lines of detection to ensure proper detection of malicious acts
  • Multiple lines of delay to increase adversary task time and complexity of adversary attacks

• Balanced Protection
  • Ensure any and all paths to a target are protected equally

• High Reliability
  • Redundant equipment
  • Contingency plans
  • Compensatory measures
Facility Design Characterization
Facility Characterization – Investigation

Investigate anything that impacts physical protection system (PPS) performance:

• Physical and environmental conditions
• Facility operations
• Facility policies and procedures
• Regulatory requirements
• Safety considerations
• Legal issues
• Corporate goals and objectives
• Facility personnel
Physical and Environmental Conditions

Weather and environment

Facility boundaries, fencing, and barriers

Building construction materials (walls, ceilings, floors, windows, and doors), rooms, and access points

Heating, ventilation, air conditioning, power distribution system, environmentally controlled areas, and locations of hazardous materials

Communication types (e.g., signal and alarm transmission)

Consult drawings and walk down facility
Facility Operations

Products and processes
  o Material in use and in storage

Operational hours
  o Normal working hours
  o Shifts during weekdays and weekends, and number of employees on shifts
  o 24 hours per day, 7 days a week

Visitors and vendors
  o Access approval process
  o Escort requirements
Facility Operations

Nuclear and other radioactive material characteristics
  o Amount, type (element and isotope), and physical form
  o Attractiveness (from NSS No.13, Table 1)

Use, storage, and staging locations

Tracking mechanisms
  o Nuclear material accounting and control
  o Unique container identification number
  o Tamper indicating or other devices

Shipping and receiving processes
Regulatory Requirements and Procedures

Regulatory requirements
- International agreements
- State and local requirements
- Regulatory authority
- Industry practice
- Building codes

Policies and procedures
- Written policies and procedures
- Training policies and procedures
- Other indications of safety and security culture
- Unwritten policies and practices
  - Interview staff
  - Observe routine work
Safety Considerations

Safety regulations and requirements

- When safety requirements conflict with security requirements, there must be an interface because the objectives are the same

- Safety and security requirements must both be considered in facility and process design

Use safety documents for information related to sabotage target analysis
Legal Issues

Depending on the State, legal issues might be the most complex and difficult to solve in physical protection:

Security liability – comply with requirements

Failure to protect – negligence liability

Overreaction – excessive use of force, invasion of privacy

Guard or response force training

Labor and employment issues – labor unions, work practices
Security Culture

Defined as characteristics, attitudes, and behavior

Management’s role in security
- Is security identified as a goal or objective?
- Identified values versus actions?

Determination of security culture
- Underlying assumptions
  - Facility viewed as attractive target?
  - Visible evidence in PPS equipment and practices?
Target Identification
Target Identification

Target: Nuclear and radioactive material or safety related systems, structures, and components (SSCs)

Unauthorized removal targets
- Nuclear materials
- Radioactive materials

Sabotage targets
- Nuclear or other radioactive materials
- Nuclear facilities or SSCs, the sabotage of which could lead to radiological consequences
# Nuclear Material Categorization

<table>
<thead>
<tr>
<th>Material</th>
<th>Form</th>
<th>Category I</th>
<th>Category II</th>
<th>Category III&lt;sup&gt;c&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Plutonium</td>
<td>Unirradiated&lt;sup&gt;b&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;b&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% $^{235}\text{U}$ or more</td>
<td>10 kg or more</td>
<td>Less than 10 kg but more than 1 kg</td>
<td>10 kg or more</td>
</tr>
<tr>
<td></td>
<td>- Uranium enriched to 10% $^{235}\text{U}$ but less than 20% $^{235}\text{U}$</td>
<td>10 kg or more</td>
<td>Less than 10 kg but more than 1 kg</td>
<td>10 kg or more</td>
</tr>
<tr>
<td></td>
<td>- Uranium enriched above natural but less than 10% $^{235}\text{U}$</td>
<td>10 kg or more</td>
<td>Less than 10 kg but more than 1 kg</td>
<td>10 kg or more</td>
</tr>
<tr>
<td>3. Uranium-233</td>
<td>Unirradiated&lt;sup&gt;b&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</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>

**Note:** This table is not to be used or interpreted independently of the text of the entire publication.

<sup>a</sup> All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

<sup>b</sup> 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.

<sup>c</sup> Quantities not falling in Category III and natural uranium; depleted uranium and thorium should be protected at least in accordance with prudent management practice.

<sup>d</sup> 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.

<sup>e</sup> 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.
Radiological Consequences

- Identify vital areas
- High Radiological Consequence (HRC) Threshold
- Graded protection requirements based on level of potential radiological consequences
- Unacceptable Radiological Consequence (URC) Threshold
- Prudent management practices to secure and control access to assets and safety-related equipment
Sabotage Considerations

NSS No.13 has no defined categorization for sabotage targets

Identifying what constitute URC and HRC thresholds is the responsibility of the State

NSS No.13 specifies sabotage protection:
- PPS should protect against any sabotage scenarios that exceed URC threshold established by the State
- PPS measures (5.20 to 5.43) that protect high-consequence facilities, including nuclear power plants, against HRC

Possible bases for URC definition
- Quantitative – safety threshold
- Qualitative – relative risk
Types of URC and HRC Thresholds

Release-based or dose-based thresholds
- Maximum allowable release or dose
- Usually use existing safety limits
- Requires detailed dispersion modeling

Design limit threshold
- Specifies an unacceptable facility state (e.g., core damage)
- Requires less analytical effort
- Generally more conservative
Sabotage Attack Type

Direct
- Gain access to area at which material is located
- Apply energy directly to material to cause dispersal
- For example, using explosives to disperse material

Indirect
- Use energy present in the material or process system to cause dispersal
- Requires
  - Initiating event; a process upset condition
  - Disabling systems designed to mitigate the upset
- For example, disabling one or more of the three essential safety functions: reactivity control, cooling, and containment
Sabotage Prevention

SSCs should be appropriately protected, following the graded approach

NSS No.13 contains requirements for high-consequence facilities, such as nuclear power plants, including locating within a vital area, inside a protected area

- Inventories of nuclear or radioactive material with potential to exceed HRC, if dispersed (direct scenarios)

- A minimum set of SSCs are needed to prevent HRC (indirect scenarios)
Power Reactor Vital Areas

Protect SSCs to ensure the continued operation of all critical safety functions

Reactivity control, including control rod (SCRAM) components and systems

Decay heat removal including control and coolant source

Process monitoring including instrumentation for pressure, coolant level, and others

Reactor coolant makeup

Support functions, including electrical power, switchgear, startup, and controls
Designing for Functional Detection
System designers must consider

- High probability of detection
- Decreased nuisance alarm rate and false alarm rate
- Decreased installation cost
- Decreased operation and maintenance cost
Classification of Interior Sensors

- Active or passive
- Covert or visible
- Volumetric or line
- Mode of application
- Boundary penetration
- Interior motion
- Proximity
Interior Sensor Requirements/Constraints

Requirements
- Probability of detection, nuisance alarm rate, adversary paths
- Likely adversary (insider, outsider, or collusion)
- Containment or denial

Constraints
- Target location
- Building construction
- Interior configuration
- Access controls
- Approved sensor lists
- Costs
Interior Sensor Engineering Applications

- **Boundary Penetration**
  - Detection at doors, windows, walls, vents, floors, ceilings, etc.
  - Detection zone easily identified

- **Interior Motion**
  - Detection in a volume of space
  - Detection volume (not visible)

- **Proximity**
  - Detection at the target
Boundary Sensor Design Considerations

Boundary
  o Wall construction
  o Ceiling construction
  o Floors
  o Ventilation
  o Doors
  o Windows
Door and Window Penetration Detection

Balanced Magnetic Switch (BMS)

Active infrared

Glass break

Break wire
Wall, Ceiling, Floor, Ventilation Protection

Break wire

Vibration sensor

Active infrared
Interior Motion Sensor Types

Microwave

Passive infrared (PIR)

Dual technology

Video motion detection (VMD)

Provide volumetric coverage of area
Basis of Entry Control – Identity Verification

Something you possess
  o Key
  o Card

Something you know
  o Personal identification number (PIN)
  o Password

Something you are
  o Biometric feature
Perimeter Intrusion Detection

Detects unauthorized access

Defines perimeter around the facility
  o Detection sectors
  o Access control point(s)
  o Delay and response features

Subsystems
  o Detection devices
  o Assessment systems
  o Communications and power distribution
Perimeter Intrusion Detection Profile

Analyze design against intrusion methods
  • Jumping
  • Crawling
  • Bridging, tunneling

Consider:
• Sensor design
• Overlaps
• Assessment
• Sector boundaries,
• Access control points
Intrusion Detection Design

High probability of detection and low nuisance and false alarm rates
Detection before delay
Tamper protection and line supervision
Response force integration
Facility-specific system design

Detection
- Integrated with delay
- Balanced approach
- Along all credible paths
- Graded approach
- I
Detection for Small Modular Reactors

• Need for reduced infrastructure to conduct intrusion detection
• Need for earlier detection technologies
Designing for Functional Delay
Delay - elements designed to slow down an adversary after they have been detected.

Delay is effective only after detection with assessment that initiates the response.
Defining delay

System detection and response time must be less than adversary task time after first alarm

- To increase system success probability
- Detect intrusion earlier
- Reduce assessment time
- Reduce response time
- Increase adversary task time
Effective Barrier Characteristics

Provides delay *immediately* after detection

Exhibits *balanced design*; no weak links

Uses *delay-in-depth*
Effective Barrier Characteristics

Provides delay *immediately* after detection

Detection with Assessment before Delay was not implemented and resulted in a successful theft
Effective Barrier Characteristics

Exhibits *balanced design*; no weak links
Effective Barrier Characteristics

Uses *delay-in-depth*
Passive vs. Active Delay

Passive Delay
Physical *fixed barriers* against both vehicle and personnel

Hardened walls, floors, and doors

Active Delay
Power required to activate
- Dispensables
  - Obscurants
  - Irritants
  - Foams
- Active barriers
  - Pop-up vehicle barriers
Adversary Capabilities Impact on Physical Protection Systems
Delay for Small Modular Reactors

• May need additional delay to allow for offsite response force strategies

• Delay cannot impede the operational ability of the site

• Delay measures cannot impact safety of site personnel

• Delay barriers may provide additional layer of containment against radiological release
Designing for Functional Response
Response Force Equipment

- Weapons
  - Unarmored
  - Armored

- Vehicles
  - Unarmored
  - Armored

- Communication Equipment
  - Radio
  - Telephone
  - Duress alarm

- Night Vision Devices
Guard and Response Force survivability considerations
  o Based on DBT capabilities
  o Facility specific

Gas Mask and Chemical / Bio Suits

Self-Contained Breathing Apparatus

Helmet

Body Armor

Intermediate Force Weapon

Vest (Tactical)

Flashlights and Binoculars
Response Considerations

Response survivability
  - Based on DBT capabilities
  - Facility specific

Improved radio systems

Protected response routes

Hardened fighting positions

Automated response capabilities

Secure equipment storage

Secure communications center

Breaching equipment

Training
Guard and Response Force Training

Critical part of protection program

Facility and target familiarization

Should include all contingencies

Should be realistic
Contingency Planning by Response

Three Planning Objectives

Planning Principles and Concepts

Interaction with Outside Agencies

Use of Force
Contingency Planning Concepts

Contingency planning concepts include:
- Identify and prioritize potential targets
- Determine appropriate response strategies for the facility
- Identify optimal guard and response configuration
- Develop plans and procedures
Response Strategies

Primary Response Strategies
  o Containment - A strategy to prevent adversaries from leaving the facility with an asset
  o Denial - A strategy to prevent adversaries from reaching an asset and completing a sabotage act

Secondary Response Strategies
  o Locate and Recover is used to pursue adversaries who have left the facility with nuclear material, regain control of it, and return it to the facility
  o Recapture is used to regain control of a critical location on the facility occupied by adversaries to prevent completion of a malicious act
Facility Recapture

Facility recapture

- Offsite response will have to work through the facility to recapture the facility
- Offsite response may have to engage with adversaries in less-than-desirable circumstances
- May require larger response force members
Response Considerations for Small Modular Reactors

• Offsite Response Forces will require some sort of denial strategies and recapture strategies

• Important to ensure that responders are adequately trained
  • Weapons
  • Tactics
  • Facility Target Locations

• Important to performance test and evaluate response time

• Response time and response strategies will be a major driver for other physical protection system functions
Engineering Analysis of
Physical Protection Systems
System Effectiveness

System effectiveness is calculated using the following equation

\[ P_E = P_I \times P_N \]

**Probability of Interruption (P_I)**
- Estimates the likelihood of an appropriate response arriving and interrupting the adversary before the task is completed

**Probability of Neutralization (P_N)**
- Estimates the likelihood of an appropriate response preventing an adversary from completing attack
Comparing Timelines

- Adversary Begins Task
- Adversary Task Time
- Sensing Opportunities
- Adversary Detected
- Response Time
- Adversary Interrupted
- Adversary Completes Task
- PPS Response Time*

*Response Force Time
Calculating Probability of Interruption

The cumulative probability of detection ($P_D$) along a path up to, and including, the Critical Detection Point (CDP)

$$P_I = 1 - [(1-P_{D_1})*(1-P_{D_2})*...*(1-P_{D,CDP})]$$

Example

$$P_I = 1 - [(1-.8)(1-.6)(1-.6)] = .97$$

Assume that the 3rd sensing opportunity is the CDP
Calculating $P_I$

Timely Detection

- A sensing opportunity on a path is timely if PPS Response Time is less than Adversary Task Time remaining after first sensing

- PPS Response Time must be less than system delay time after first alarm to achieve adversary interruption

- Only timely detection along the adversary path contributes to $P_I$

Critical Detection Point (CDP)

- Last sensing opportunity along a path where PPS Response Time is less than the Adversary Task Time remaining after first sensing
Calculating $P_1$ (continued)

Using adversary and PPS timelines to find the CDP

[Diagram showing timelines for adversary task time, adversary task time remaining after first sensing, and PPS response time, with labels for timely and not timely sensing opportunities.]
Analysis Methods and Tools

Analysis can be based on manual methods
- Single-path analysis
- Scenario-based analysis
- Tabletop tactical analysis

Analysis can be computer-based
- Multi-path analysis
- Modeling and simulation systems

Analysis can incorporate performance testing
- Limited scope performance tests (LSPTs)
- Force-on-force exercises
P_N Concepts

P_N is a component of the overall effectiveness of a PPS
  - Measures effectiveness of response after interruption

Simple methods to measure P_N require data about:
  - Threat numbers, capabilities, and equipment
  - Response numbers, capabilities, and equipment

More complex methods require data about:
  - Initial locations, deployment routes, final locations of response force and adversaries
  - Terrain, building schematics, PPS characteristics
Neutralization Analysis

$P_N$ is the second factor in system effectiveness

Wide range of methods to determine $P_N$
- Expert judgment
- Mathematical models
  - Simulations
- Actual engagements

Trade-off is accuracy vs. cost

This course uses a simple numerical method emphasizing number of adversaries and responders with equal capabilities
Engineering Approach to Probability of Neutralization

Engineering for probability of neutralization must consider the factors affecting probability of neutralization.

Engineers must ask the following questions:
- Will there be a difference in the probability during daylight and nighttime?
- Will there be a difference in the probability in inclement weather?
- Does neutralization analysis need to be conducted for all of the potential adversary pathways?

Considering these questions leads to improved understanding of the probability of neutralization.
Engineering Approach to Probability of Neutralization (continued)
Probability of Neutralization ($P_N$)

**Probability of Neutralization ($P_N$)** - The probability that once a threat is interrupted, the response force can prevent a threat from completing unauthorized removal of nuclear material or sabotage of a nuclear facility.

Mathematically, $P_N$ is:

$$P_N = \frac{N_{\text{wins}}}{N_{\text{engagements}}}$$

Assuming:

- $N_{\text{engagements}}$ is a statistically significant number of engagements
- All engagements have the same initial conditions
- Two possible outcomes per engagement: win or loss

$P_N$ can be estimated by using any one of several methodologies.
What I wish I knew about nuclear security: Panel Discussion