

Workshop

Malaysians



SAND No. 2008-3832C
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.





Basics of Systematic, Risk-based Approaches to Facility Security

Nancy B. Jackson, PhD

International Chemical Threat Reduction Department
Sandia National Laboratories



Facility Security Helps Avoid Undesirable Consequences

- **Death/Severe Injury**
- **Chemical contamination**
 - People
 - Environment
- **Political Instability**
- **Economic Loss**
- **Industrial capacity loss**
- **Negative public psychological effect**
- **Adverse media coverage**





Many kinds of chemical facilities need to be secured

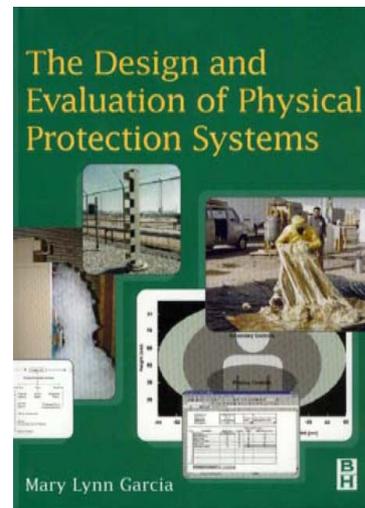


- **Small-scale research laboratories**
 - Many different chemicals used in small amounts
- **Large-scale manufacturing plants**
 - Limited types of chemicals used in large amounts
- **Security measures need to match facility and threat**
 - Can't afford to defend against all imaginable threats



Systematic approaches to facility security

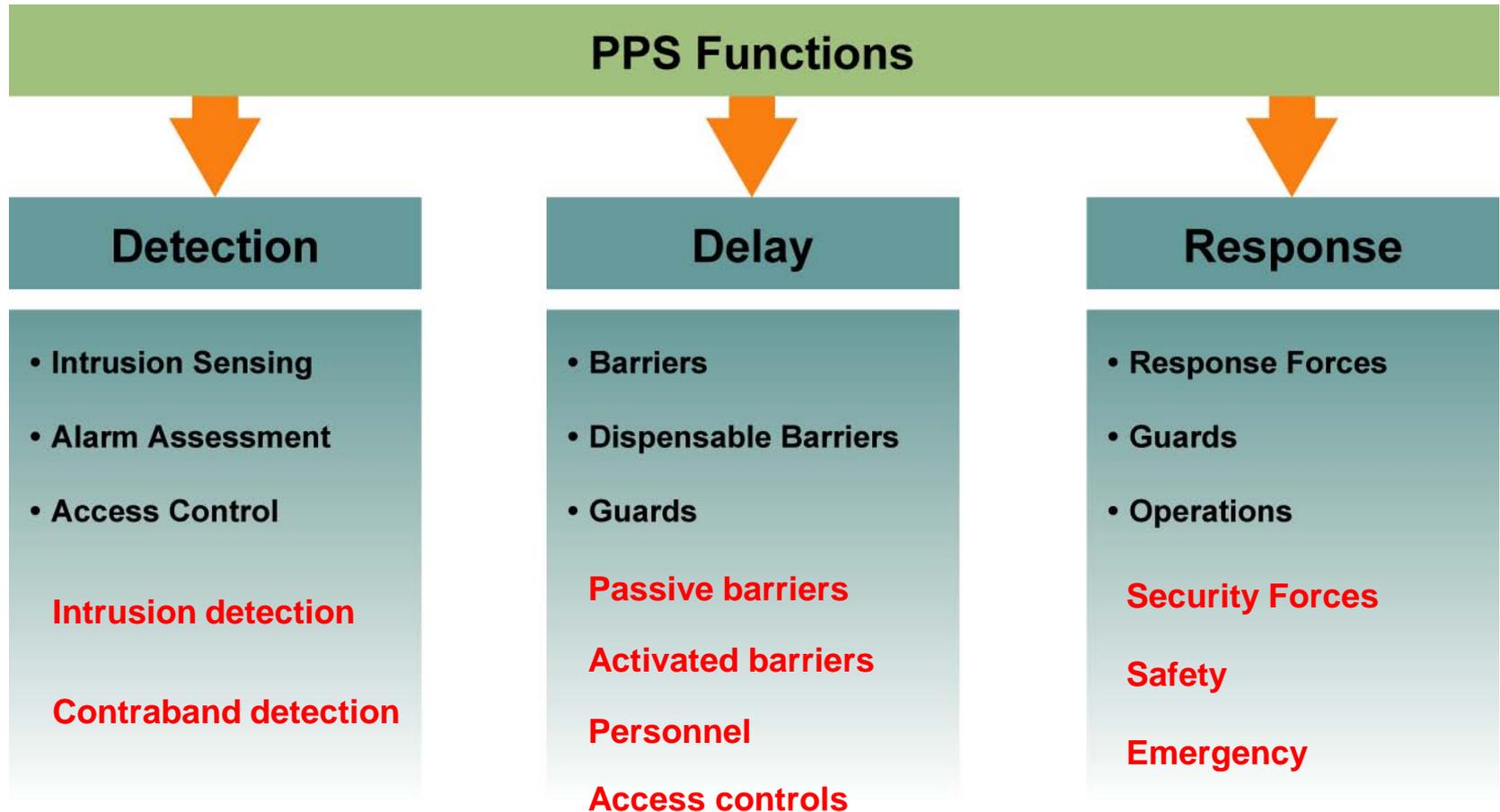
- **Balance risks**
- **Systematically decide what operational practices or equipment purchases will be most effective**
- **Originally developed for designing physical security systems for high-value items**
 - **Nuclear facilities**
- **Methodology applied to other high-value facilities**
 - **Large chemical plants**
 - **Electric power plants and transmission lines**
 - **Water treatment plants**



<http://www.sandia.gov/ram/>



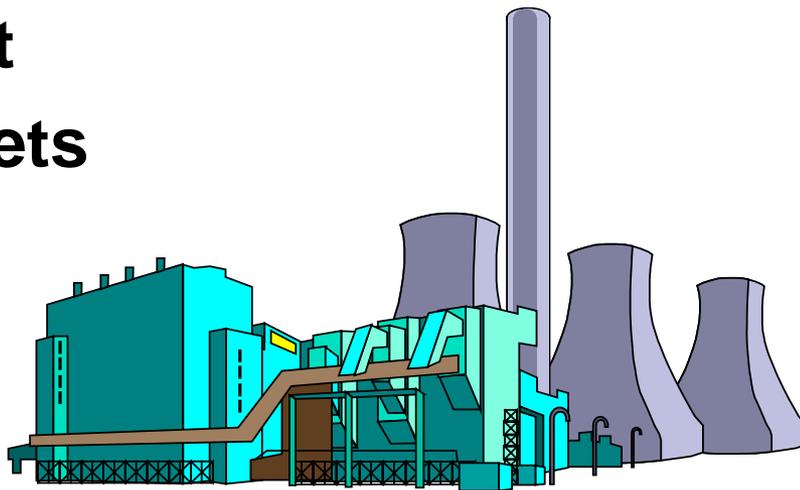
What should a Protection *SYSTEM* do?





Protection System Design Objectives

- **Understand what to protect and from whom:**
 - **Characterize the facility**
 - **Define the threat**
 - **Identify the targets**





Facility Characterization

- **Characterize the facility considering:**
 - **Mission**
 - **Operations**
 - **Budget**
 - **Safety**
 - **Legal Issues**
 - **Regulatory Issues**





Facility Characterization

- **Characterize the facility in terms of**
 - **Site boundary**
 - **Buildings (construction and HVAC systems)**
 - **Room locations**
 - **Access points**
 - **Processes within the facility**
 - **Existing Protection Systems**
 - **Operating conditions (working hours, off-hours, potential emergencies)**
 - **Safety considerations**
 - **Types and numbers of employees**
 - **Legal and regulatory issues**



Facility Characterization

- **Facility characterization provides important data that will:**
 - **Help identify locations and assets to be protected**
 - **Provide important details about the facility that will allow system designers to make design selections**
 - **Establish what existing Protection System components are already present at the facility**
 - **Document facility layout for use in analysis**



Design Basis Threat

- **Design Basis Threat (DBT) is the attributes and characteristics of potential adversaries, who might attempt unauthorized removal of sensitive material or sabotage, against which a physical protection system is designed and evaluated.**
- **At the national level, the DBT is typically defined by the government.**
- **At the facility level, also:**
 - **Consider local threats**
 - **Local criminals, terrorists, protestors**
 - **Consider insider threats**
 - **Employees and others with access**



Threat Definition

- **Using all information sources determine:**

Classes of adversaries

Outsiders—no authorized access

Insiders—authorized access

Collusion—between Outsiders and Insiders





What Might Motivate Adversaries?

- **Terrorists**

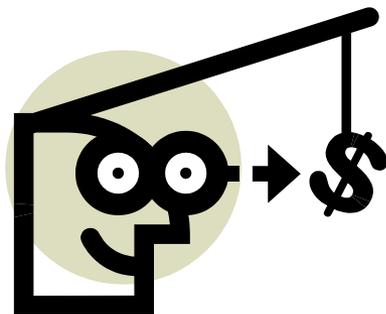
- Ideology

- **Criminals**

- Financial

- **Activists**

- Ideology



- **Insiders**

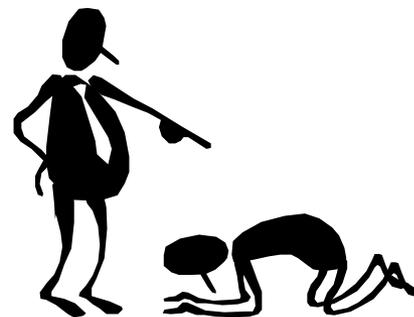
- Ego

- Ideology

- Revenge

- Financial

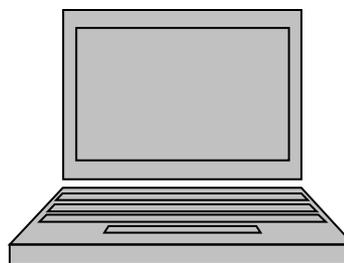
- Coercion





Target Identification

- Determine the possible targets for the following actions:
 - Sabotage
 - Identify vital areas to protect
 - Theft of material or information
 - Identify location of material to protect





Systems are designed to protect specific targets against specific threats

- **Targets**
 - Facility targets exist
 - Undesirable theft or sabotage consequences
- **Threats**
 - National / International level threats
 - Local threats

Consequences + Threats = Need for protection



The Main Question

- How much risk is acceptable versus the cost of reducing that risk?
- Must manage multiple risks in a holistic manner
 - Financial
 - Liability
 - Health and safety
 - Business/mission
 - Security





Concept of Risk

- Risk associated with adversary attack is a function of:
 - Severity of consequences of an event
 - Likelihood of adversary attack
 - Likelihood of adversary success in causing an undesired event
- Risk is a relative ranking not an absolute number
- Combines three relevant factors into a single parameter
- Allows comparisons of threat, security system, and consequence variations
- Helps in prioritizing/justifying requirements and budgeting (efficient allocation of resources)



Risk, Risk Assessment, and Vulnerability Assessment

- **Risk – *Measure*** of the potential damage to, or loss of, an asset based on the probability of an undesired event
- **Risk Assessment – *Process*** of analyzing threats to, and vulnerability of, a facility; determining the potential for losses; and identifying cost-effective corrective measures
- **Vulnerability Assessment – *Process*** in which qualitative/quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a security system



Risk Management

- **Risk mitigation usually includes a combination of:**
 - **Avoidance**
 - **Reduction**
 - **Spreading**
 - **Transfer**
 - **Acceptance**
- **Depend on specific facility and location**



Quantify Security Risk

- **Three components:**
 - **Likelihood of attack (P_A)**
 - **Likelihood the Protection System will NOT stop the adversary ($1 - P_I \times P_N$), where**
 - P_I = Probability of interrupting adversary
 - P_N = Probability of neutralizing adversary
- **Consequences of a successful attack (C)**

$$\text{Risk} = P_A \times (1 - P_I \times P_N) \times C$$



Likelihood of Attack (P_A)

- Difficult to determine
- May be extremely low
- If worst case is assumed
 - $P_A = 1$ (assume there will be an attack)
 - Risk number is then “conditional” and risk equation becomes

$$\text{Risk} = (1 - P_I \times P_N) \times C$$



P_A Based On:

- Value of asset
- Usefulness to adversary
- Publicity value
- Availability
- Number of incidents at the installation or in the geographical area in the past
- Perceived regard for law enforcement
- Aggressor's perception of the possibility of success



Consequence (C)

- Quantifies the severity of occurrence of an event
- Number between 0 and 1
- If we assume protection is for the most critical assets, which might have a consequence value of 1.0, the risk equation becomes

$$\text{Risk} = (1 - P_I \times P_N)$$



Protective System Probabilities

- **Probability of interruption P_i**
 - The probability that the system will be able to detect and the response force interrupt the adversary
 - Computed as the cumulative detection probability along an adversary path
- **Probability of Neutralization P_N**
 - The probability that the Response Force will intercept, capture, or cause the adversary to flee



System Effectiveness

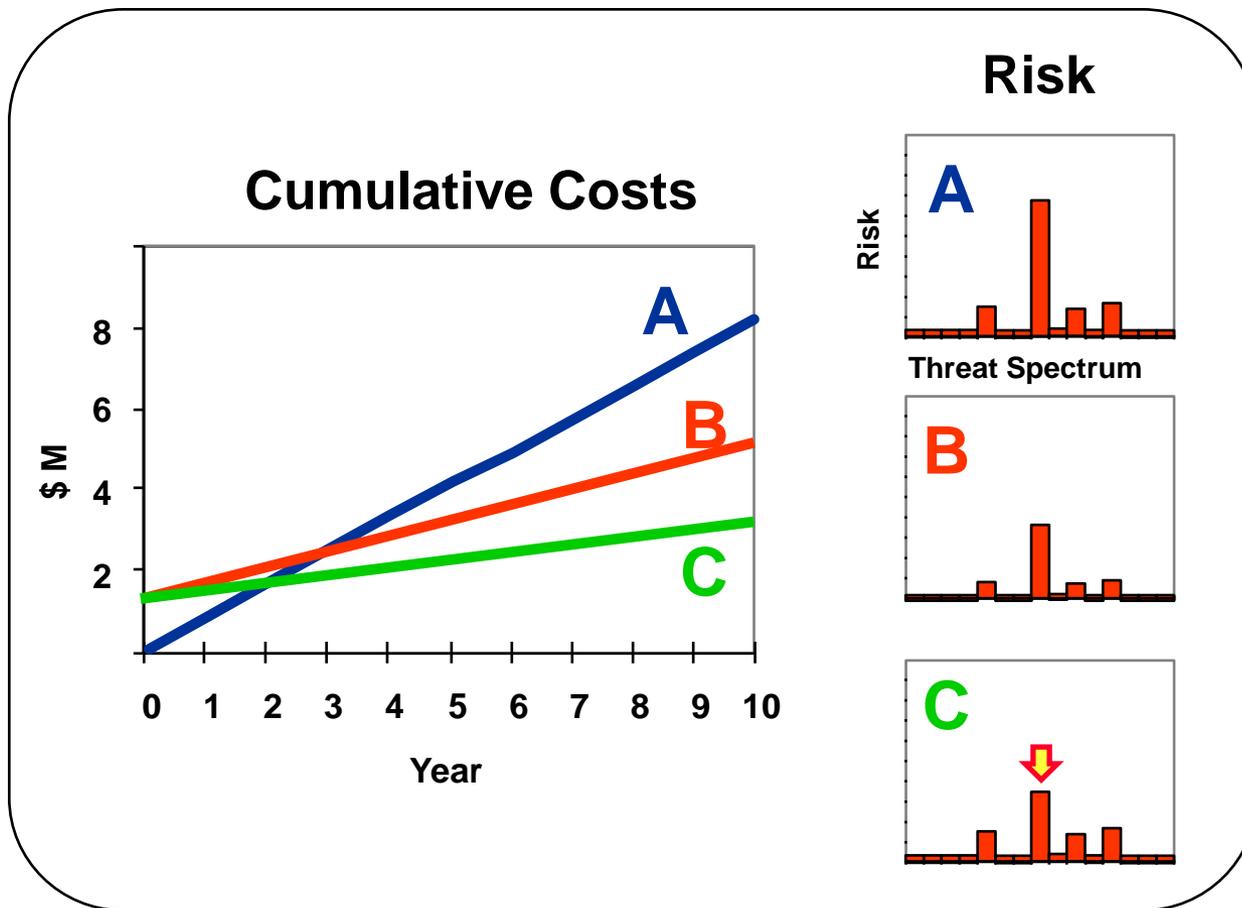
- **Probability of Protection System effectiveness is $P_I \times P_N$**
 - Derived from system modeling
 - A number between 0 and 1

$$\text{Risk} = (1 - P_I \times P_N)$$

- Residual risk after allowing for protection system effectiveness

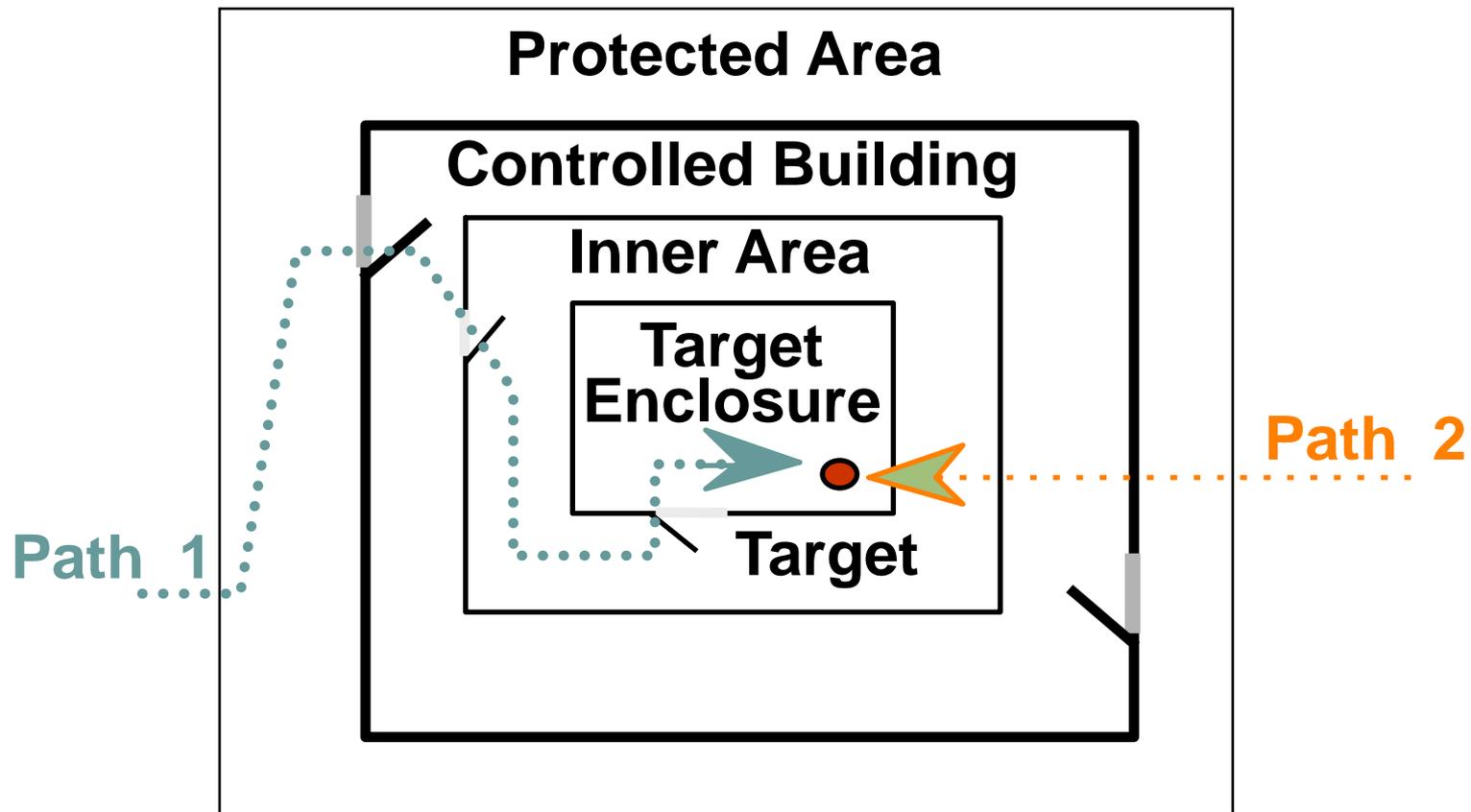


Cost Versus Risk



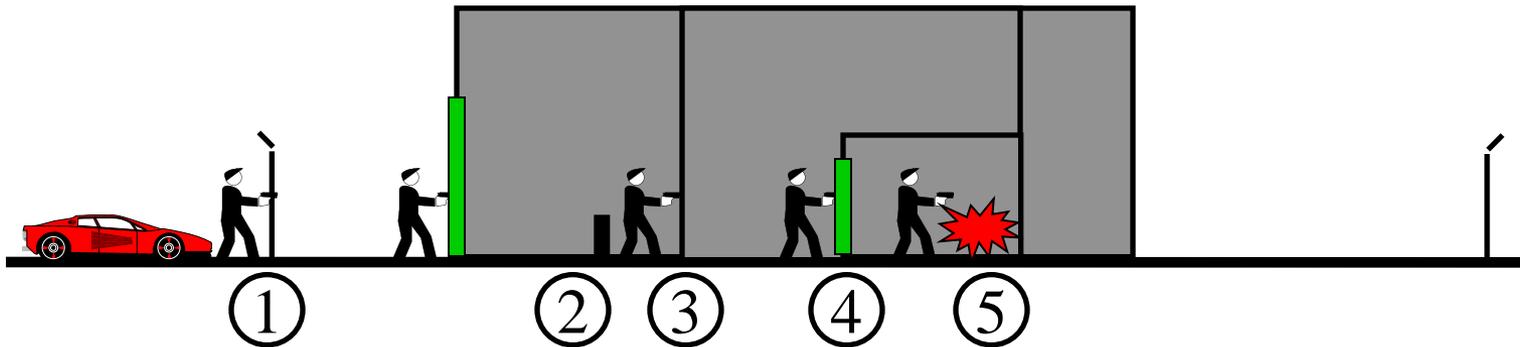


Multiple Adversary Paths to Target





Single Path Example

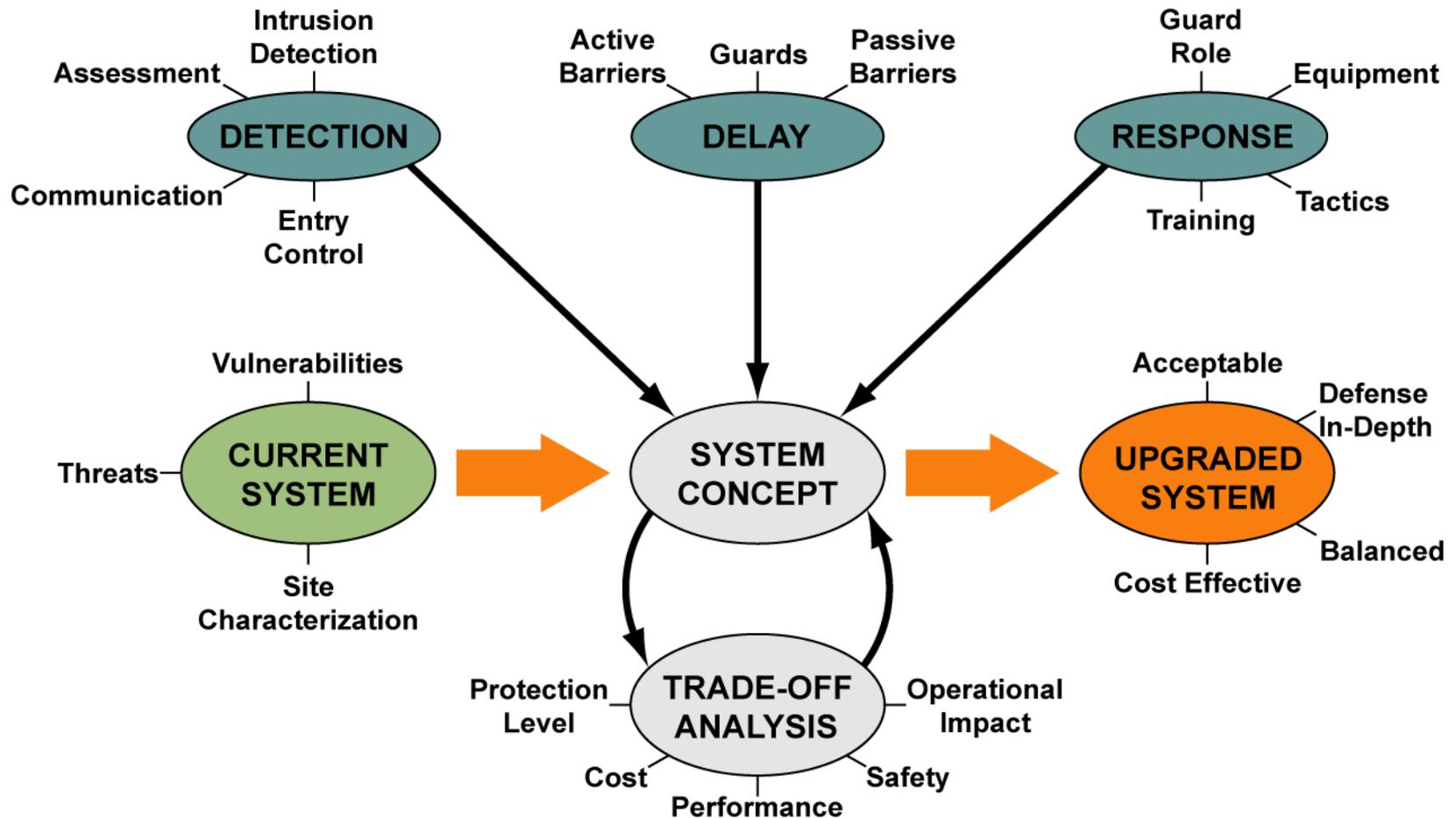


#. Action (Probability of Detection, Delay Time)

1. Penetrate fence (0.1, 10s)
2. Penetrate outer door (0.1, 15s)
3. Penetrate wall (0.5, 60s)
4. Penetrate inner door (0.1, 20s)
5. Sabotage target (0.9, 300s)



System Integration





Components of Chemical Security and Relationships Between Chemical Safety and Security

Pauline Ho, PhD

International Chemical Threat Reduction Department
Sandia National Laboratories



Chemical Security

- **Is your Department secure?**
- **How easy would it be for someone to steal chemicals?**
- **Are your chemistry stockrooms, classrooms and research labs always locked and secure?**
- **Is someone always there when these rooms are open?**
- **Do you check your orders when chemicals arrive to be sure some chemicals are not missing?**





Components of Chemical Security

- Physical security of site
- Personnel management
- Information security
- Management of chemical security activities
- Allocation of chemical security responsibilities
- Development of emergency plans
- Chemical security training



Goal: Ensure that you don't accidentally help a criminal or a terrorist get dangerous chemicals



Chemical Security: Physical Site

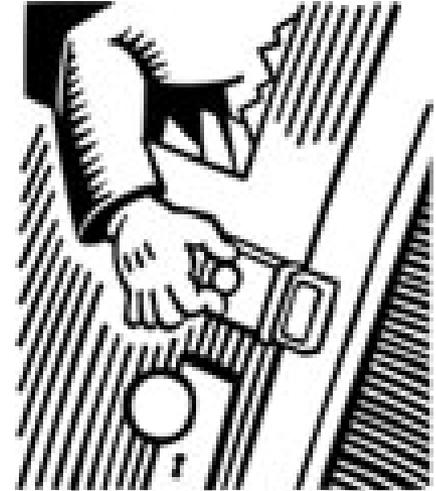
LOCK UP!!



Controlled drugs

Chemical Surety Agents

Highly toxic chemicals





Chemical Security: Personnel Management

- **Guard against both Insider and Outsider threat**
- **Does anyone check on people entering the building?**
- **Who has keys? How do they get authorized?**
 - Building
 - Stockroom
 - Individual Labs
- **When someone leaves, do you make sure they turn in keys?**
- **Don't want people making duplicate keys**





Chemical Security: Information security

- **How do you track chemical inventory?**
 - Is the information secured so unauthorized people can't read it or alter it?
- **Would you know if:**
 - some toxic chemicals disappeared overnight?
 - some toxic chemicals didn't arrive?
 - someone was ordering chemicals in the name of your institution but diverting them?

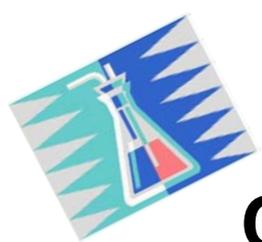




Chemical Security: Assign Responsibilities

- **Identify people who will be responsible for various chemical security activities**
 - Physical security and building modifications
 - Chemical tracking and reporting
 - Personnel and access management
 - Information management
 - Emergency planning
- **Ensure that they have the time and resources to do the job**
- **Integrate with chemical safety responsibilities**





Chemical Security: Professional behavior

- A Chemical Professional needs to use their scientific knowledge in a responsible manner



- A Chemical Educator needs to train their students to use their scientific knowledge in a responsible manner



Relationships between chemical safety and security

- **Chemical safety**: Protect against accidents
- **Chemical security**: Protect against deliberate harm
- Many practices are the same for chemical safety and security
- But there are a few areas of conflict





Good practices for both chemical safety and security

- **Minimize use of hazardous chemicals**
 - Replace with less-hazardous chemicals, if possible
 - Reduce scale of experiments
- **Minimize supply of hazardous chemicals on hand**
- **Restrict access to hazardous chemicals**
 - Know what you have
 - Know how to store, handle and dispose of what you have
 - Know who has access to materials, knowledge and expertise
- **Plan what to do in an emergency**



Conflicts between chemical safety and security: Information Sharing

Science generally means sharing information widely, but this may not always be advisable

- **Safety**

- Label everything so people can recognize hazardous chemicals.
- Alert community and especially emergency responders to possible chemical dangers.
- Share knowledge about chemical hazards so people know to be alert.

- **Security**

- Labels help identify targets for theft or attack.
- Sharing locations of chemicals can publicize targets for theft or attack.
- Sharing knowledge of chemical hazards could inspire harmful behavior (copy-cat criminals).



Conflicts between chemical safety and security: Facility exits

- Locking exit doors is secure, but not safe.
 - For **safety**, we want people to be able to leave the facility quickly and by many routes.
 - For **security**, we want to control exits as well as entrances so chemicals (or equipment) don't get taken.





Setting priorities

- **Labs need to be **safe**, **secure** and **productive****
 - Policies and practices need to be flexible enough to allow for the uncertainties of research.
 - Policies and practices need to align with local laws, regulations, practices and culture. Can't just copy policies from somewhere else.
- **Use risk-based security and safety measures.**
 - Can't afford to defend against every imaginable hazard.
 - Identify threats, characterize facilities, identify alternatives, analyze costs vs. performance
- **Be alert for suspicious activities or inquiries**



Summary

- **Chemical safety and security are important**
 - **Academic chemistry laboratories are an attractive target for theft of chemicals**
- **Chemical safety and security measures have a lot of overlap**
 - **Attitudes and awareness**
 - **Policies**
 - **Physical additions/changes to buildings and labs**





Workshop evaluation and feedback form

- Please help us improve this workshop by filling out and returning this form.





Thanks for coming!

- This work was funded by the U.S. Department of State Chemical Security Engagement Program
- We thank
 - Loretta Humble
 - Steve Iveson
 - Ruth Bitsui
 - Jessica Jones
 - Nelson Couch, PhD

