SAND2010-0704C

Physical Security Systems Engineering

Presented by

Felicia A. Durán
Principal Member of Technical Staff
Sandia National Laboratories – Security Systems Analysis Department
☎ 505-844-4495 💻 faduran@sandia.gov

University of Missouri INMM Student Chapter Workshop
February 10, 2010 • Columbia, MO

Sandia National Laboratories 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. Unclassified/Unlimited Release SAND2010-XXXXC.

Sandia National Laboratories

Sandia National Laboratories Overview

- **A multi-program R&D laboratory of the U.S. Department of Energy**
- **Managed and operated by Sandia Corporation**
  - A subsidiary of Lockheed Martin Corporation
- **~8,500 employees**
- **~$2 billion annual budget**
- **Major locations**
  - Albuquerque, New Mexico
  - Livermore, California

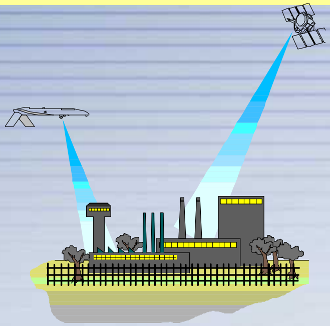
Sandia National Laboratories

SNL is a National Security Laboratory

Sustain Nuclear Weapons Stockpile

Safe, Secure, Reliable Weapons

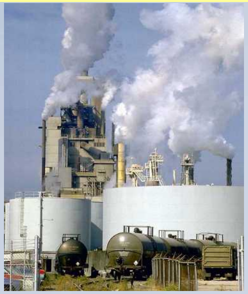
Reduce Vulnerability to Weapons of Mass Destruction



Detection

Surveillance

Advance Surety of Global Infrastructures



Energy

Information

Transportation

Enhance National Security Measures

Anti-crime and anti-terrorism technology

Smart Weapons

Sandia National Laboratories

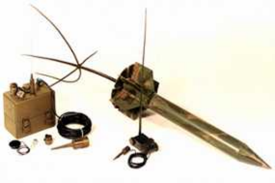
SNL Security Capabilities

- Intrusion detection lab and test field
- Access control and contraband detection lab
- Physical protection test area
- Force-on-force simulation laboratory
- Development and conduct of system vulnerability and risk assessments
  - Nuclear facilities
  - Infrastructure, cyber
  - Water utilities, dams, communities, prisons, chemical facilities
- Training courses

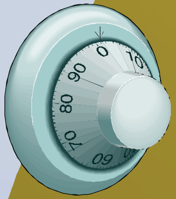
Sandia National Laboratories

Security Systems Development

1960



- Counter Insurgency
- Intrusion Detectors



- Control

1970

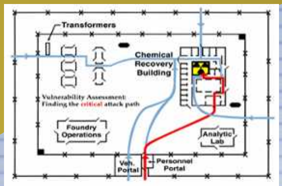
- Safe Secure Trailers
- Future Look
- Embassy Upgrades
- Accident Response Container

1980

- Pantex and NATO Upgrades

- Weapon Access Denial System

1990



Transformers
Chemical Recovery Building
Vulnerability Assessment: Finding the critical attack path
Foundry Operations
Analytic Lab
Veh. Portal
Personnel Portal

- Vulnerability Assessments

- FSU Security Support

- Deployable Systems

2000

- Intrinsic Security

- Insider

- Pu Management
- Cooperative Security
- Bilateral Transparency

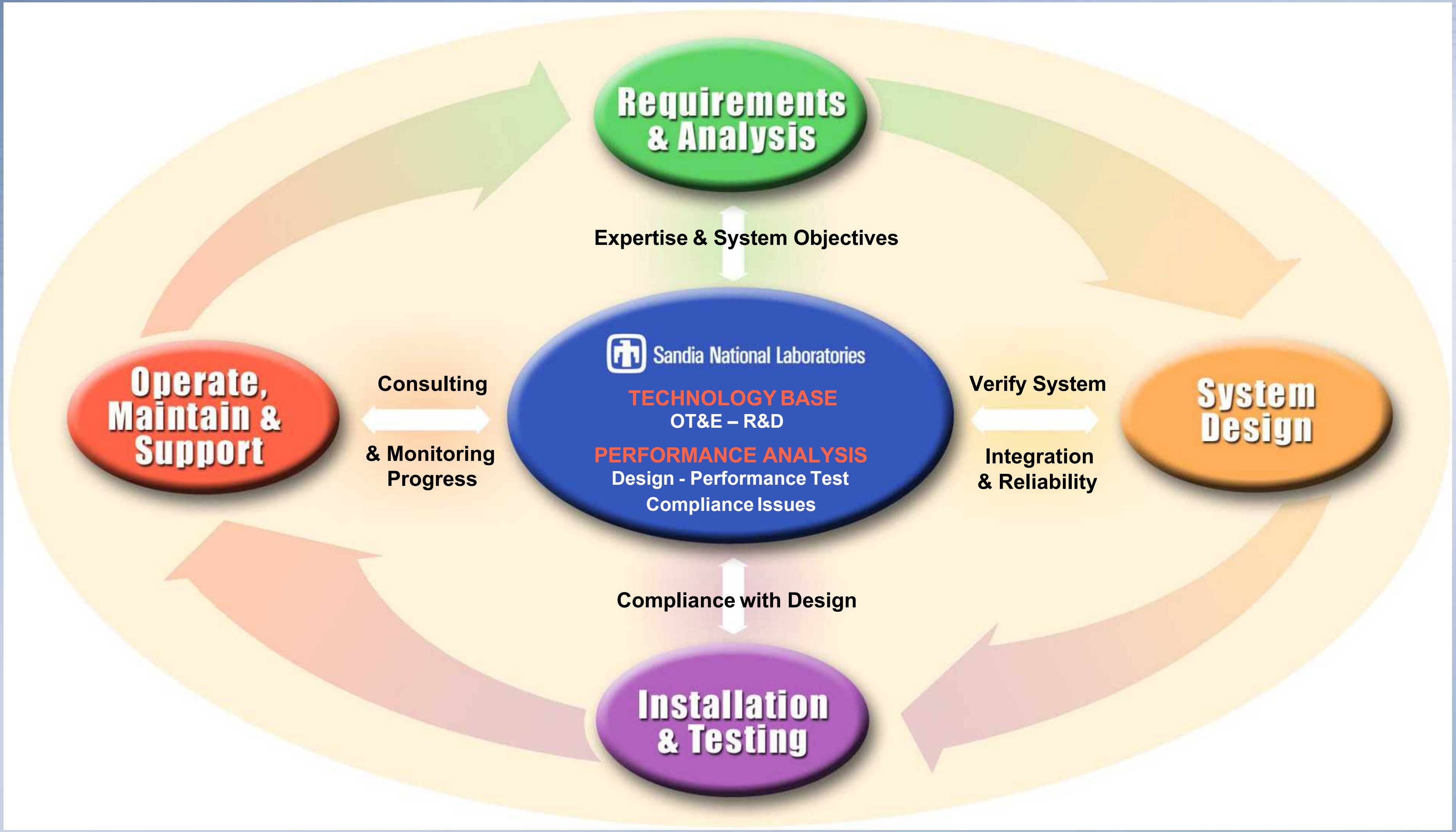
2010

- Dynamic Security

- C^{4}I

- Advance Denial
- Remote Response
- Integrated Surety

Security Systems Engineering Approach



Requirements & Analysis

Expertise & System Objectives

Sandia National Laboratories

TECHNOLOGY BASE

OT&E – R&D

PERFORMANCE ANALYSIS

Design - Performance Test

Compliance Issues

Operate, Maintain & Support

Consulting

& Monitoring Progress

Verify System

Integration & Reliability

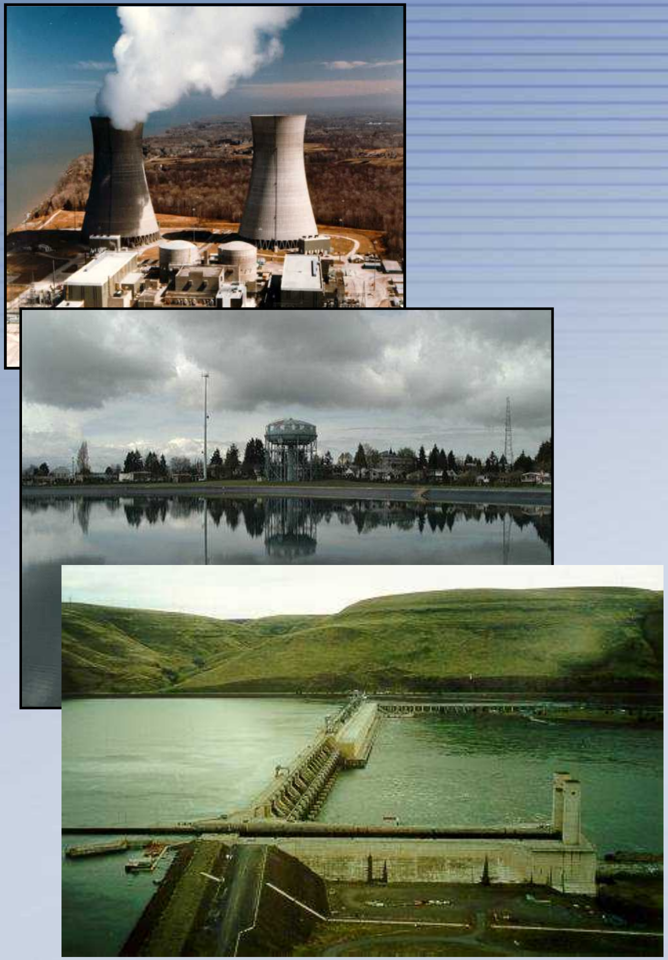
System Design

Compliance with Design

Installation & Testing

Sandia National Laboratories

Sandia Physical Security Activities



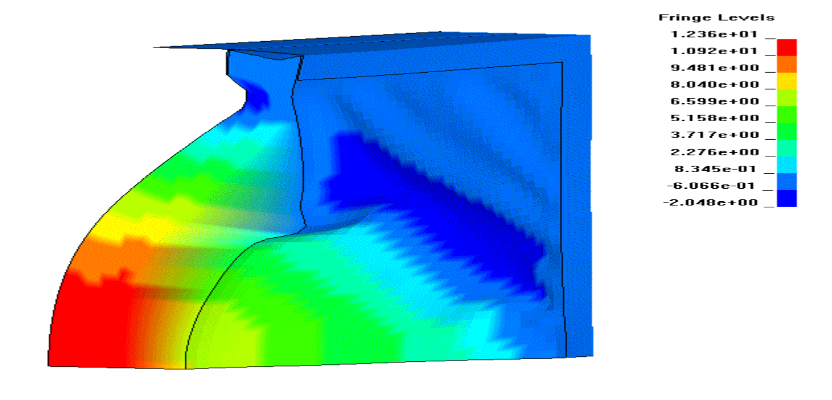
- **DOE and NNSA’s Lead Laboratory for Physical Security**
  - Primary Security Systems Engineering Organization
  - Site interface for gap analysis, R&D, implementation
- **Security/Vulnerability Assessment and Physical Protection Systems for DOD, OFAs, State/Local and Private Industry**
  - Lead Design Agent for the Navy’s Strategic Weapons Security system
  - Technical design agency and integrator of all NNSA Office of Security Transportation Systems including authorization basis (safety and security) for operation
  - Other Facilities of National Importance
    - Nuclear Power Plants, Critical Infrastructures
- **Nuclear Emergency Response Program for DOE**
- **International Physical Security Programs for DOE/NA-24**

Related Nuclear Fuel Cycle Work

NRC Basic Security Course
Train NRC and State Inspectors

NPP VA
Apply process to support security improvements

MOX Fuel Facility
Explosives Effects Analysis



Columbia Generating Station
Joint Conflict And Tactical Simulation Analysis

Definitions

- **Physical Protection System (PPS) — an integrated system of equipment, personnel, and procedures designed to protect selected assets**
  - Also Physical Security System (PSS), Physical Security, Security
- **Vulnerability Analysis (VA) — A systematic, performance-based process that is used to evaluate the ability of a physical security system to meet performance requirements**
- **System – A combination of interacting elements organized to achieve one or more stated purposes**
- **Systems Engineering – An interdisciplinary approach and means to enable the realization of successful systems**
  - Customer needs and required functionality
  - Documentation of requirements
  - Design and system validation for complete problem
  - Business and technical needs
  - Quality product to meet user needs

References: Garcia, "Vulnerability Assessment of Physical Protection Systems," Butterworth-Heinemann, Woburn, MA, 2001; Systems Engineering Handbook, INCOSE, 2007.

Sandia National Laboratories

Physical Security
Risk Equation and Timeline

P(Attack) *P(Adversary Success)* *Consequences*

$$\boxed{\text{Risk} = P_A \cdot [\overbrace{1 - \underbrace{P_E}_{P_I \;\; P_N}}^{}] \cdot C}$$

P(Interruption) *P(Neutralization)*

Pre-Incident	t_0 Incident	Post-Incident
$\{P_A(1- P_E)C\}$	$\{(1- P_E)C\}$	$\{C\}$
Policy Changes	Detection	Emergency Response
Technology Options	Delay	Mission
Personnel Options	First Response	Business
Planning Requirements		Loss of Life
		Costs
		Public Reaction
		Recovery

Why Use Risk Analysis in Systems Engineering?

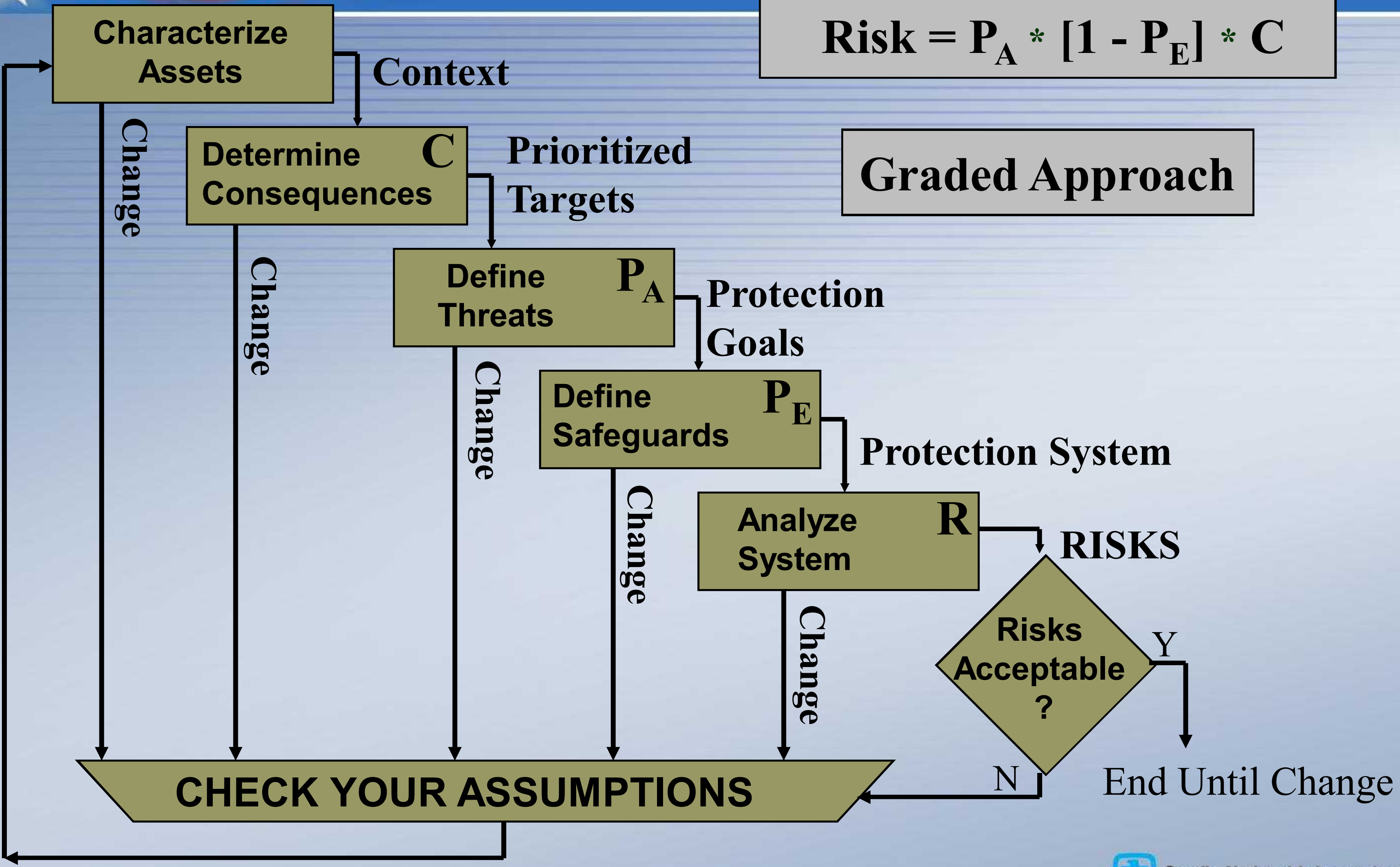
- **Understand a system or operation better**
  - What consequences can occur? How severe can they be?
  - How can they occur? What are their root causes?
  - What are we relying on to prevent them?
  - How often do these causes and effects occur?
- **Understand the costs & benefits of alternatives**
  - How do different design or operational alternatives affect the consequences and/or root causes?
    - Lower magnitude? Lower likelihood?
    - What is the cost to reduce risk? Is it worth it?
- **The ultimate objective of risk analysis is always to support some sort of decision.**

Sandia National Laboratories

Security Risk Assessment Process

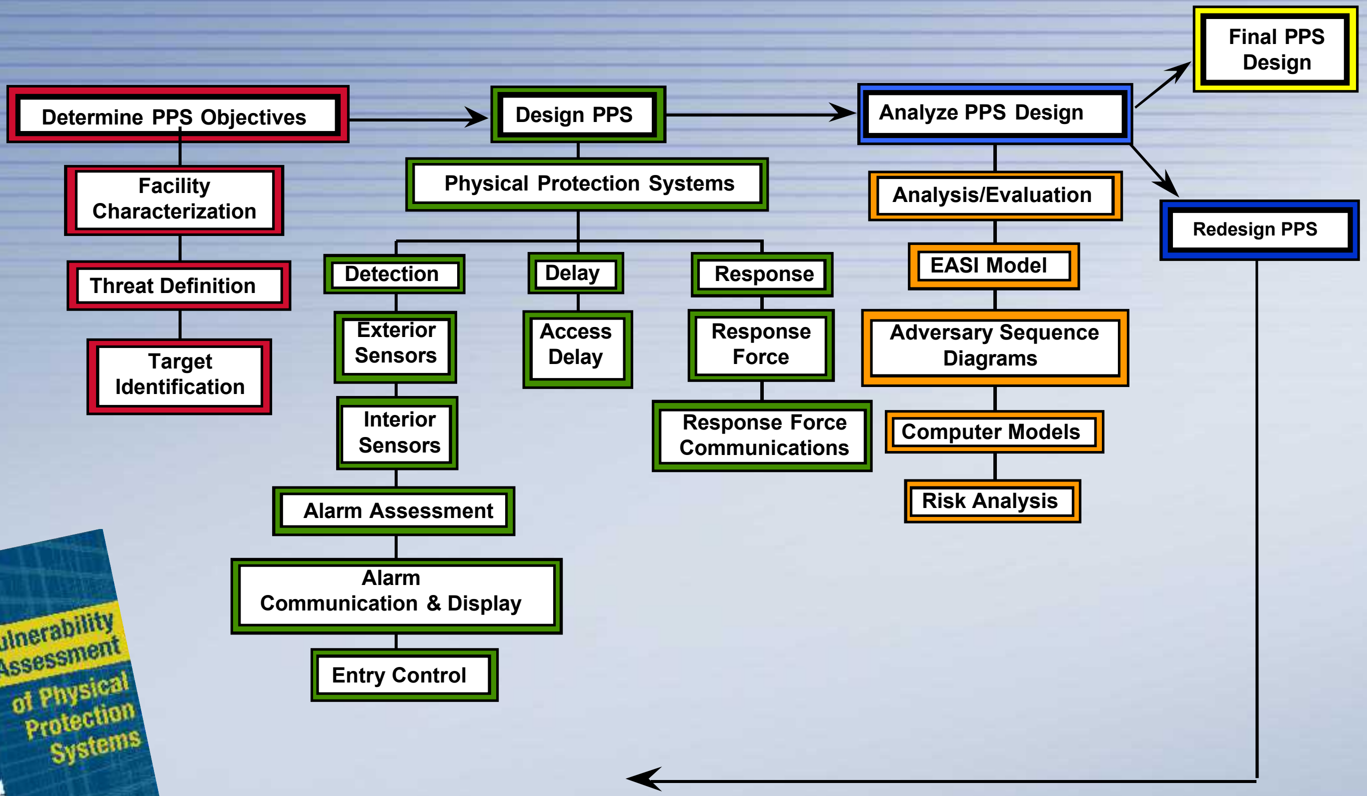
$$\text{Risk} = P_A * [1 - P_E] * C$$

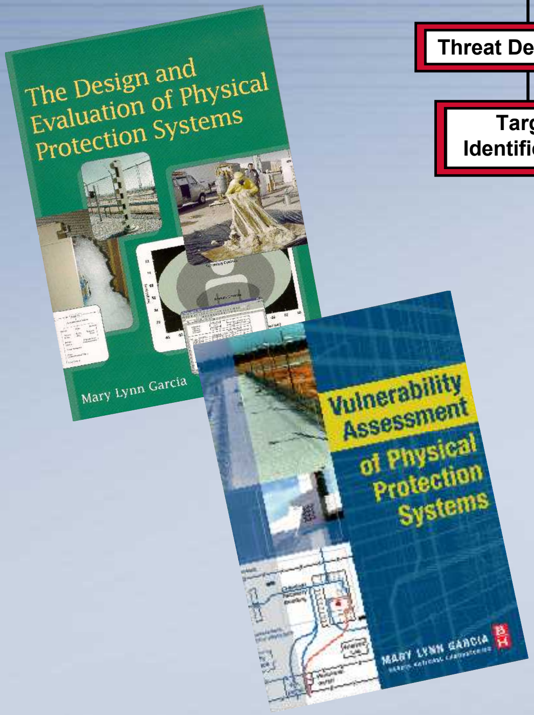
Graded Approach



Sandia National Laboratories

Security Design and Evaluation Process Outline (DEPO)

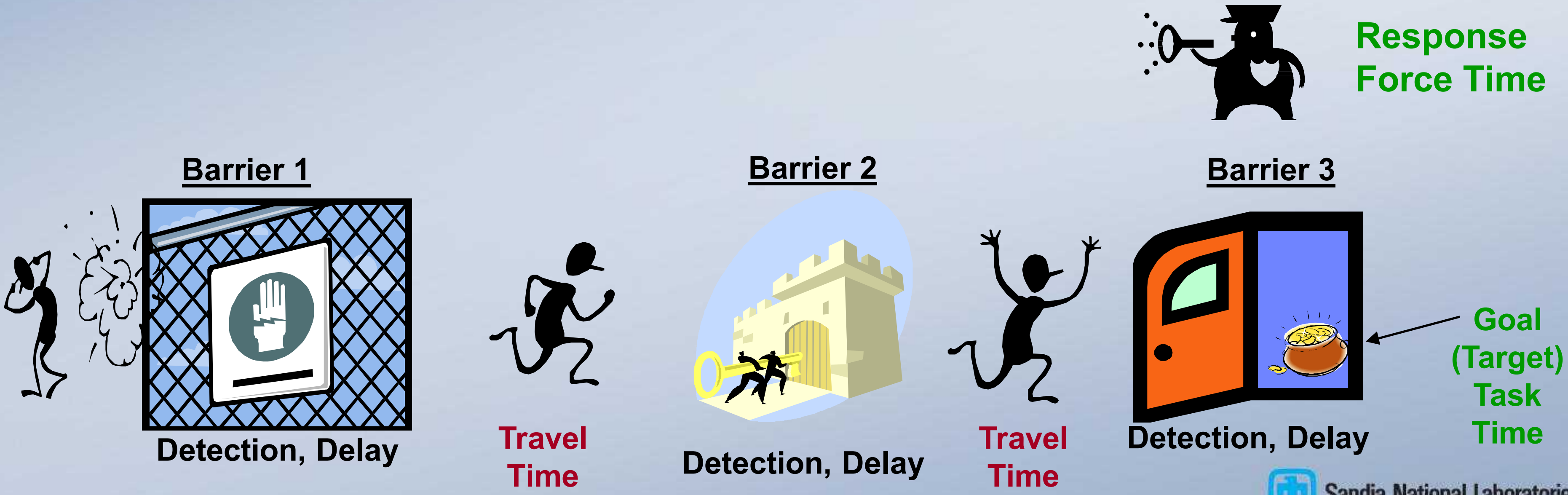



The Design and Evaluation of Physical Protection Systems
Mary Lynn Garcia
Vulnerability Assessment of Physical Protection Systems
MARY LYNN GARCIA

Sandia National Laboratories

Assessment of Physical Security Systems

- **Evaluation is based on "timely detection"**
  - Can the good guys respond before the bad guys accomplish their goal?
    - Each barrier has a task time (delay) and probability of detection
    - Bad guys' optimal path depends on which elements can be defeated, given their physical attack skills and tools



Response Force Time

Barrier 1

Detection, Delay

Travel Time

Barrier 2

Detection, Delay

Travel Time

Barrier 3

Detection, Delay

Goal (Target) Task Time

Characteristics of Adversaries

- **Many different adversaries, each w/different goals**
  - Terrorist, criminal, activist, disgruntled customer, vandal, psychotic, opportunist (e.g., “attractive nuisance”)
- **Characteristics vary by adversary or group**
  - Capability: Available tools (skills, weapons, etc.), knowledge, number of attackers, facility access, authority, etc.
  - Tactics: force, stealth, deceit, combinations thereof
  - Intent: Why are they attacking? What do they want to accomplish in their attack?
  - Motivation: What are they willing to sacrifice to make the attack succeed? Will they die for it? Get arrested? …
- **Adversaries vary by location & target**
  - Info about adversaries by location & target available from law enforcement (local, state, FBI, Joint Terrorism Task Force, …)
  - Info about international groups is hard to obtain without connections to the intelligence community

Reference: Garcia, “Vulnerability Assessment of Physical Protection Systems,” Butterworth-Heinemann, Woburn, MA, 2001.

Characteristics of Adversaries (cont.)

- **Which adversaries should we defend against?**
  - Depends on the consequence potential and consequence mitigation options
    - Low consequences ➔ do nothing or buy insurance
    - Catastrophic ➔ defend vs. terrorists or use redundancy
- **Deterrence is real but hard to quantify**
  - Most rational adversaries won’t attack if they don’t believe they will win. So… most real attacks succeed!
  - How do I measure why I have never been attacked?
- **Pre-Attack detection helps high-security sites**
  - Elaborate attacks are risky for adversaries to prepare
    - Easy attacks ➔ common tools, few people ➔ small footprint ➔ hard to detect beforehand
    - Elaborate attacks ➔ legally controlled tools, many people ➔ larger footprint ➔ easier to detect beforehand
  - Defenders must “raise the stakes” for adversary planning

Sandia National Laboratories

Characteristics of Insider Adversaries

- **Motive: Why an insider takes malevolent actions**
  - Malevolent when hired ➔ pre-employment screening
  - Becomes malevolent after being hired: motives include revenge, romance, profit, financial problems, new friends, new beliefs, thrill of "being a spy"
    - Often hard to tell btw. malevolence & legitimate activities
- **Means & Opportunity: How an insider operates**
  - Knowledge: insider may know rules, procedures, detection methods, vulnerabilities, defense strategies, locations of key systems or assets…
  - Access: solo physical or cyber access to key systems, locations, equipment or information
  - Authority: ability to manipulate records or order others to do (or refrain from) tasks that effect attack scenario
  - Each class of employee has different knowledge, access and authority, so they will have different attack options.

Reference: Garcia, "Vulnerability Assessment of Physical Protection Systems," Butterworth-Heinemann, Woburn, MA, 2001.

Collusion and Other Insider Attack Methods

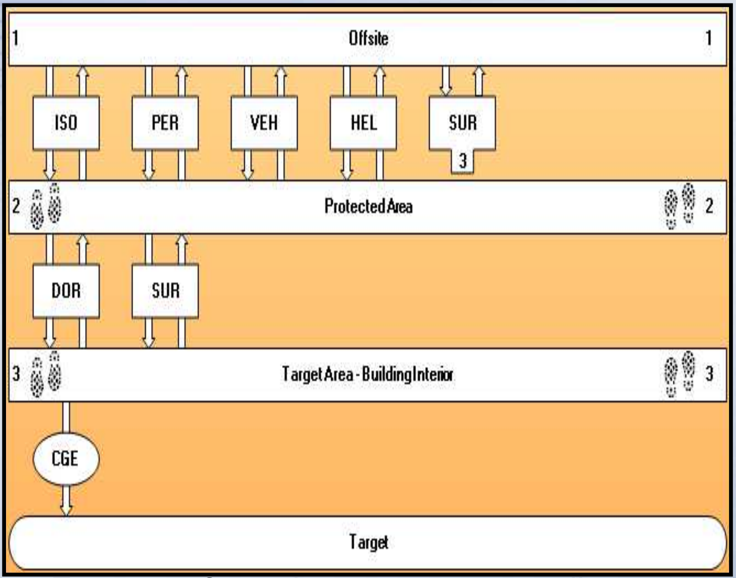
- **Passive vs. Active Insider Attacks**
  - Passive: insider provides information to outside attackers, but does not participate in the attack
  - Active: insider participates in the attack (violent or not)
- **Discontinuous Actions**
  - Execute attack steps as opportunities present themselves
    - Disable detector today, get target during special visit next week, remove from building during fire drill next month…
- **Protracted Theft**
  - An insider may steal a lot by stealing a little bit every day
- **Collusion: a defender’s nightmare scenario**
  - With outsiders: e.g., disable security system before attack
  - Among insiders: very common in financial crimes
    - Often most devastating – bypass many operational controls

Reference: Brackney and Anderson, “Understanding the Insider Threat, Proceedings of a March 2004 Workshop,” RAND Corporation, Santa Monica, CA, 2004.

Sandia National Laboratories

Path Analysis and Timely Detection

- **Objective: understand the most vulnerable attack paths and whether an attack can be interrupted.**
- **“Timely Detection” means the attack is detected in time for security forces to respond and interrupt it.**
  - Attack detection: How likely? At what step?
  - Who wins race btw. good guys & bad guys?
    - How long does the adversary take to complete his attack after he is detected?
    - How long does it take for a sufficient response force to arrive and engage the adversary?
- **“Path Analysis” searches all adversary attack paths & ranks them by likelihood of timely detection.**
  - Adversary Sequence Diagram models ingress & egress paths
    - Detection probability, task delay modeled for each barrier
  - Automated search for optimal (most vulnerable) paths



Example of an adversary sequence diagram.

Reference: Garcia, “The Design and Evaluation of Physical Protection Systems,” Butterworth-Heinemann, Woburn, MA, 2001.

Battle Simulation

- **Objective: understand whether a response force can win the battle & neutralize the attack force**
  - Battle doesn’t happen unless timely detection occurs
  - Looking for PN = Pr{enemy neutralized | attack detected}
- **Tools for simulating battles include**
  - Mock battles (e.g., exercises, “sand table” assessments)
  - Battlefield simulation software
    - Human-in-the loop: almost as expensive as mock battles
    - Fully automated: stochastic discrete event simulation with human behavior embodied in rule sets
- **Hard to get statistically valid estimates for PN.**
  - Too few trials to be statistically significant
  - Humans learn in repeated trials ➔ not statistically independent
  - Fully automated: hard to validate human behavior rule sets
  - PN estimates often rely heavily on expert judgment

JCATS Algorithm User's Guide, UCRL-SM-213123, Lawrence Livermore National Laboratory, Livermore, CA.

Integrating Security with…

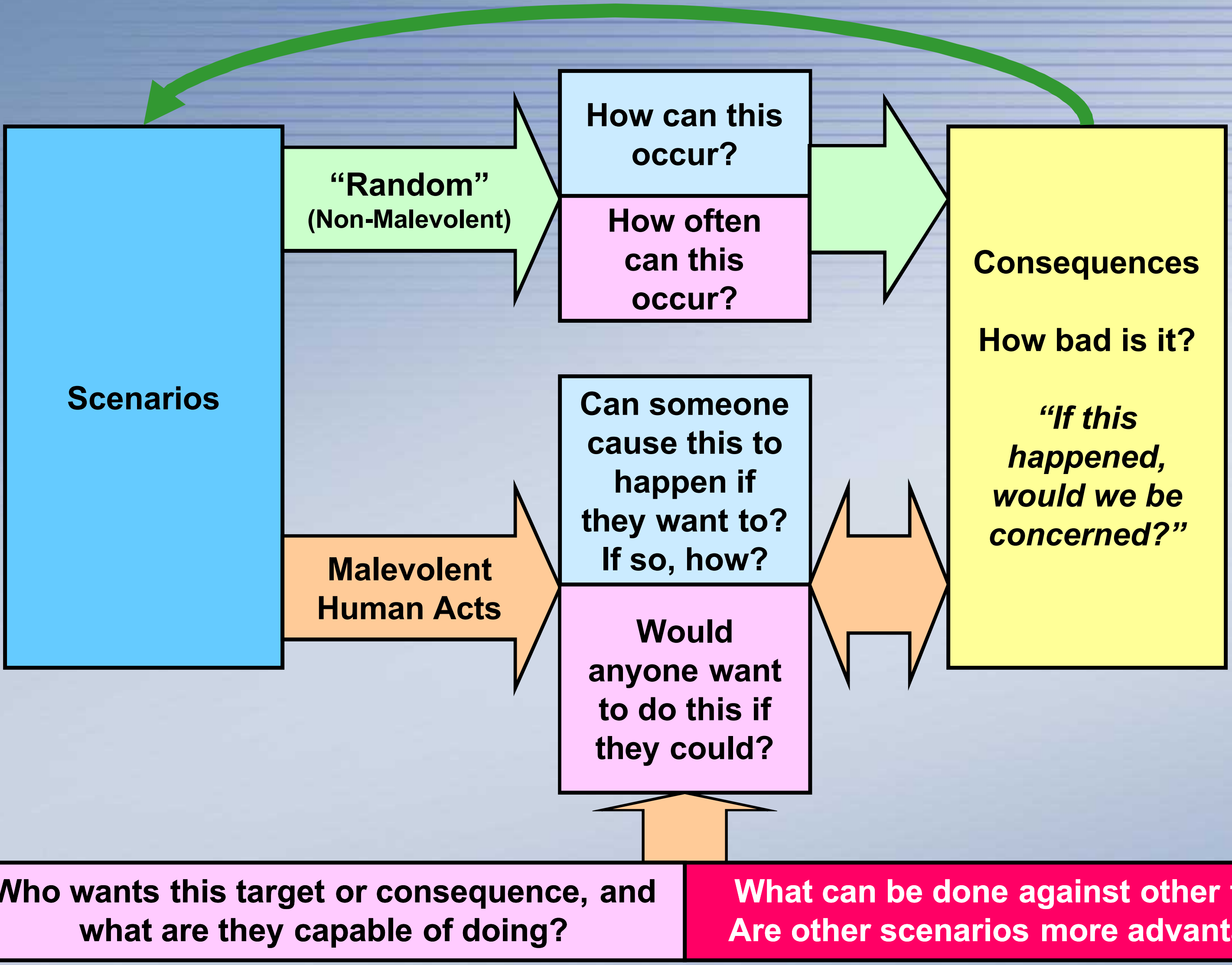
- **Traditional approaches have addressed many of our systems of concern separately.**
  - Facility safety and security
    - Random Event – Accident Progression – Consequence
    - Malevolent Threat – Vulnerability – Consequence
  - Physical and cyber security
  - Safeguards and security
- **With escalating threats and security costs, we need to address integration for more effective systems.**
  - Security and safeguards design at earliest facility concepts – Safeguards by Design
  - Leverage system functions and take credit for all the systems and operations that contribute to security
  - Move toward “intrinsic” security – We want to be secure with minimal security
- **Systems Engineering methods must be employed to achieve effective systems integration.**

Integrating Security and Safety

- **We currently make trades between safety and security**
  - Sometimes consequence level trumps all
  - Sometimes advocacy drives trade-off decisions
- **We must balance security and safety**
  - Value placed on each is subjective – “comparable risk” depends on a multitude of factors
  - Managed integration of information “stovepipes” is essential for effective and efficient solutions
- **Evaluation of Risk is common in both disciplines**
  - We can’t mathematically compare the risks
  - Objective, comparable risk metrics do not exist
  - Reason lies in the details of the risk evaluation methods…

Sandia National Laboratories

Comparison Between Safety and Security Risk Assessment



Scenarios

"Random" (Non-Malevolent)

How can this occur?

How often can this occur?

Malevolent Human Acts

Can someone cause this to happen if they want to? If so, how?

Would anyone want to do this if they could?

Consequences

How bad is it?

"If this happened, would we be concerned?"

Who wants this target or consequence, and what are they capable of doing?

What can be done against other targets? Are other scenarios more advantageous?

Results

Risk

The potential for realizing adverse consequences

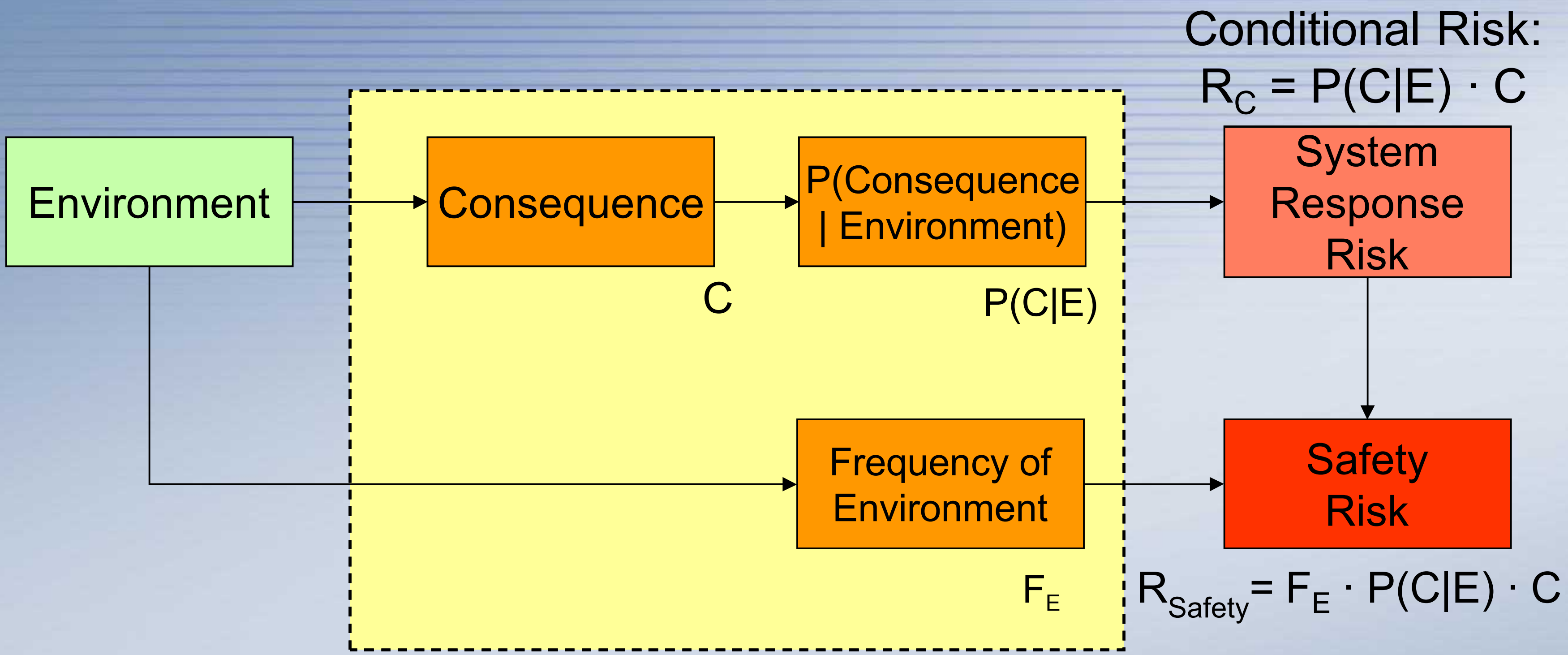
Risk Assessment

Give a judgment about the importance or significance of risk

Risk Management

Understand and accept, control, or mitigate risk

Safety Risk Calculation



Conditional Risk:

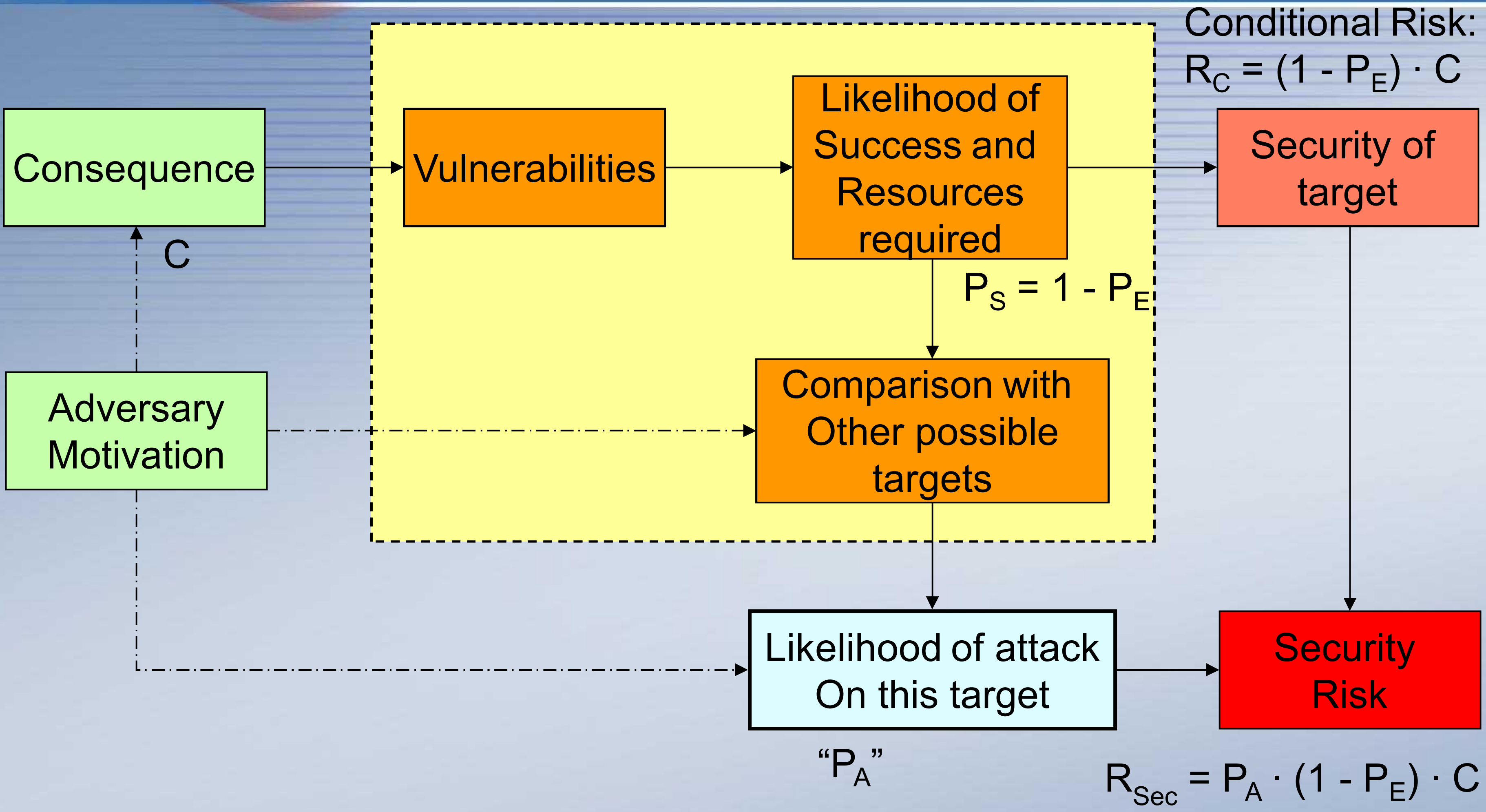
$R_C = P(C|E) \cdot C$

$R_{Safety} = F_E \cdot P(C|E) \cdot C$

Frequency of the Environment is an Independent Variable

Sandia National Laboratories

Security Risk Calculation


Consequence
Vulnerabilities
Likelihood of Success and Resources required
Security of target
C
Adversary Motivation
Comparison with Other possible targets
Likelihood of attack On this target
Security Risk
"P_A"

Conditional Risk:
$R_C = (1 - P_E) \cdot C$

$P_S = 1 - P_E$

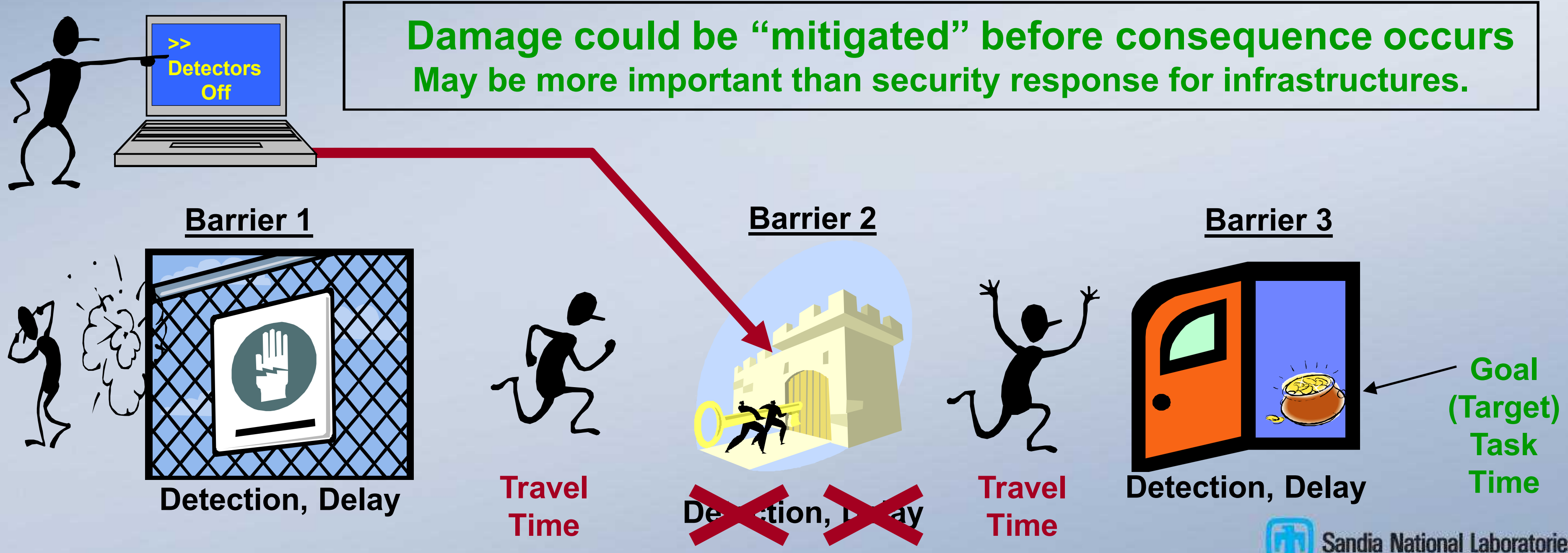
$R_{Sec} = P_A \cdot (1 - P_E) \cdot C$

Likelihood of Attack <u>Depends</u> on All Other Security Variables

Sandia National Laboratories

Assessment of Blended Security Systems

- **Cyber attacks can disable security elements before physical attack starts**
  - Shut off security delay or detection elements, then…
    … defeat "hobbled" physical security system
  - Bad guys' optimal path depends on which physical and cyber elements can be defeated, given their cyber and physical attack skills

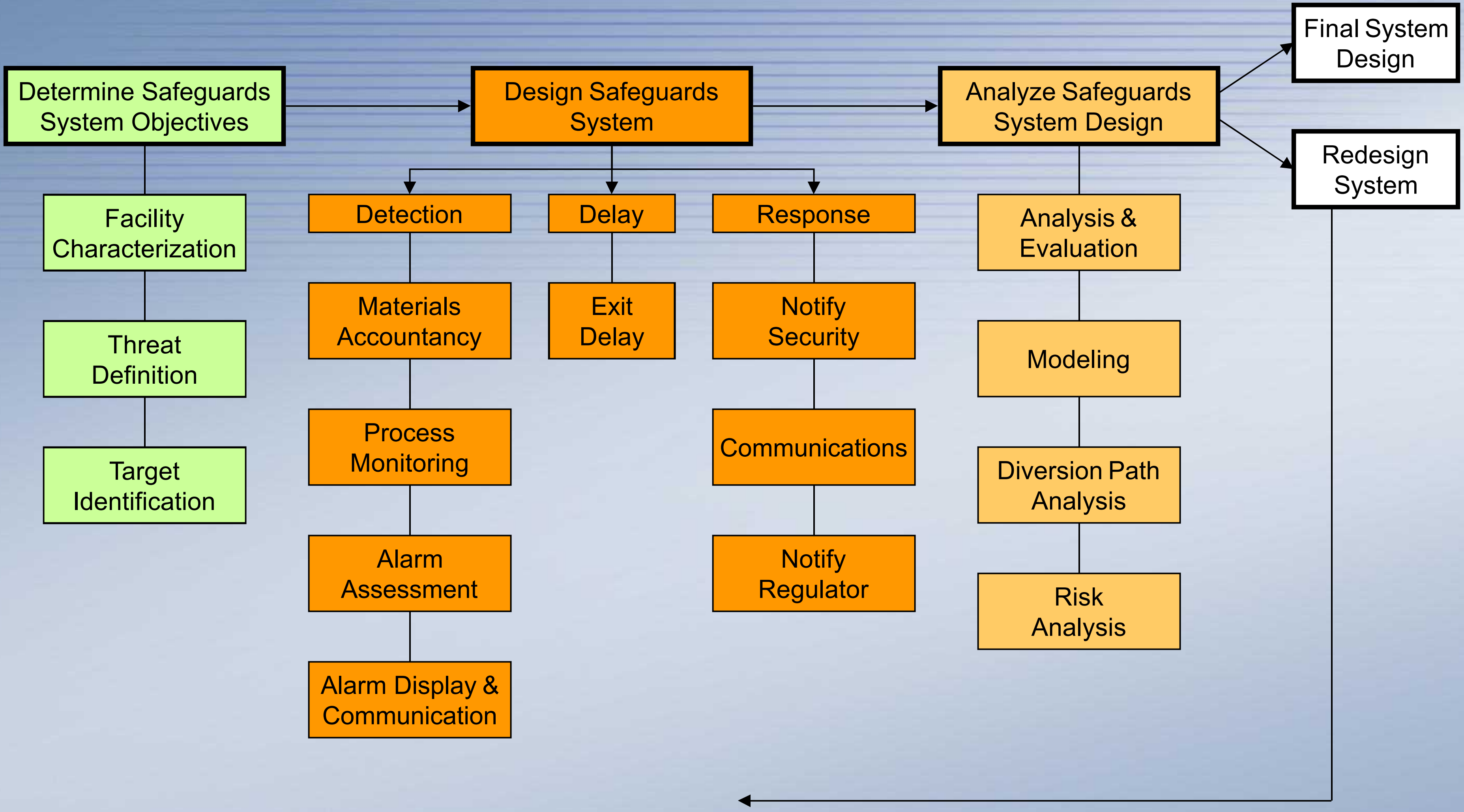


Damage could be "mitigated" before consequence occurs

May be more important than security response for infrastructures.

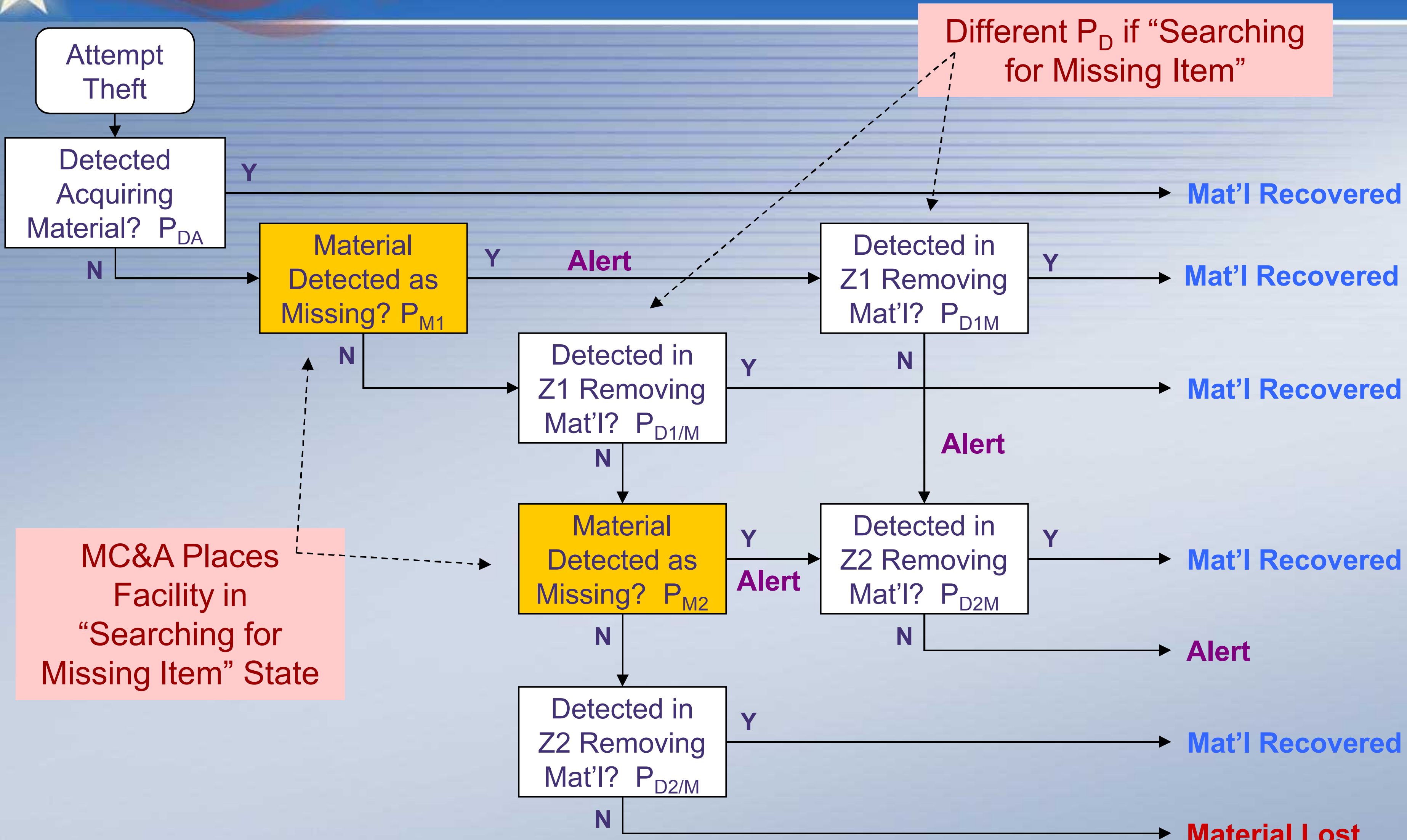
Sandia National Laboratories

A Systems Engineering Process for the Design of Safeguards Systems



Reference: Durán & Cipiti, "A Systems Engineering Process for Safeguards Design," INMM Annual Meeting (patterned after DEPO for physical security), 2009.

Integrating MC&A Operations with Physical Security – Event Sequence Diagram



Different P_D if "Searching for Missing Item"
Attempt Theft
Detected Acquiring Material? P_{DA}
Y
Mat'l Recovered
N
Material Detected as Missing? P_{M1}
Y
Alert
Detected in Z1 Removing Mat'l? P_{D1M}
Y
Mat'l Recovered
N
Detected in Z1 Removing Mat'l? $P_{D1/M}$
Y
N
Mat'l Recovered
Alert
N
Material Detected as Missing? P_{M2}
Y
Alert
Detected in Z2 Removing Mat'l? P_{D2M}
Y
Mat'l Recovered
N
N
Alert
MC&A Places Facility in "Searching for Missing Item" State
Detected in Z2 Removing Mat'l? $P_{D2/M}$
Y
Mat'l Recovered
N
Material Lost

Reference: Durán & Wyss, "Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials," INMM Annual Meetings, 2007, 2008, 2010.

Sandia National Laboratories

Intrinsic Security

- **Common definition and principles**
- **How can we be secure with minimal security?**
- **Principles for intrinsic security**
  - Defense-in-depth
  - Resiliency
  - Lifecycle Awareness
  - Balanced protection
  - Management of trust
  - Security-by-default
  - Leverage
- **Focus on mission, consequences and concept of operations**
  - Eliminate or mitigate consequences
  - Increase adversary’s difficulty of attack

Reference: Walter et al., “An Intrinsic Security Design and Assessment Methodology,” INMM Annual Meeting, 2009.

Sandia National Laboratories

Security System Engineering Opportunities

- **Fieldwork and analysis**
  - System design and evaluation, performance testing, deployment
- **Methodology development**
  - Systems engineering, risk analysis, software development, policy and requirements support
- **Equipment development**
  - Sensors, detectors, barriers, alarm communications and display, entry control, contraband detection, surveillance
  - Performance testing
- **Project management and leadership**
  - Customer relations – DOE, DOD, NRC, DHS, commercial industry and law enforcement
  - International programs
- **Training**
  - Instructors for courses and workshops

Security System Engineering Capabilities

- **Basic job pre-requisites**
  - Excellent analytical and problem-solving skills
  - Engineering, science or policy background
- **On-the-Job Training**
  - Project work
  - Customer requirements
    - DOE orders, DOD requirements, NRC regulations, IAEA
  - DEPO training – system design and vulnerability assessment
    - Garcia text books, Professional Meetings
  - National Training Center courses
- **University courses and programs**
  - Systems engineering – www.INCOSE.org
  - National security
- **Student internships**
  - Specific opportunities at www.sandia.gov/careers
  - Other National Laboratories, DOE, IAEA

Sandia National Laboratories