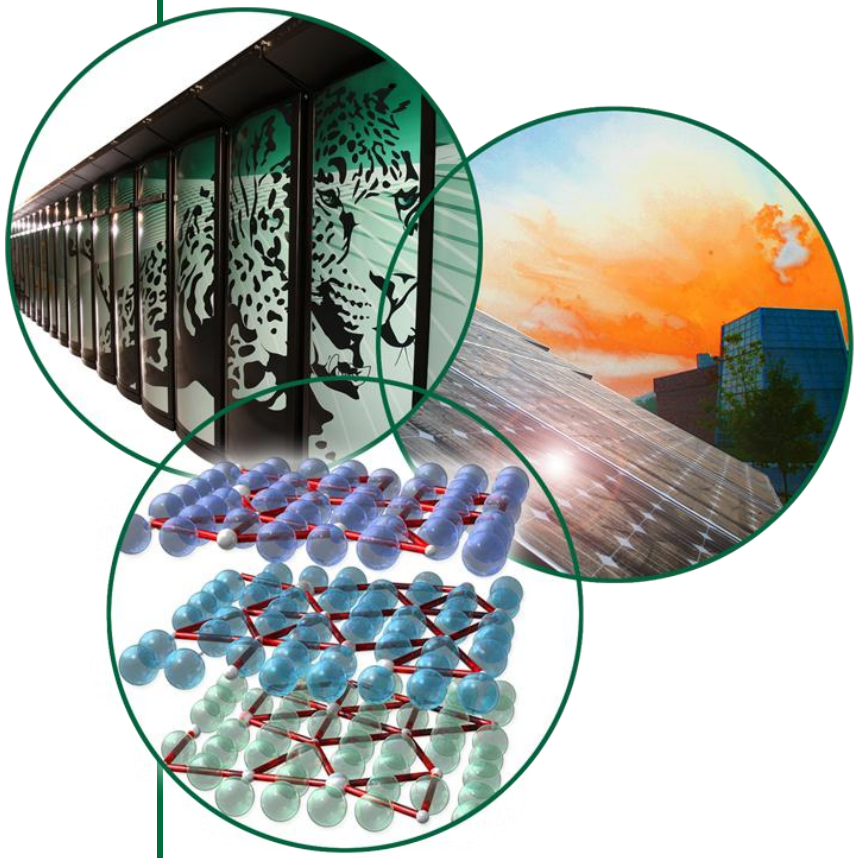
Developing the Next Generation Safeguards and Security Specialist

WINS Conference

Dyrk Greenhalgh
Oak Ridge National Laboratory

February, 2011



U.S. DEPARTMENT OF ENERGY

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

Next Generation Safeguards and Security Specialist Workshop Outline

- Facilitator introduction
- Course objectives and overview
- Definitions
- Physical security/Material Protection, Control, and Accounting (MPC&A) presentations
- Summary, questions and answers

Facilitator Introductions

- **Dyrk Greenhalgh**
  Vulnerability Assessment Team Lead
  Oak Ridge National Laboratory

Course Objectives and Overview

- Introduce safeguards and security as a practice/profession/knowledge area
- Share information on security and safeguards and management of nuclear materials
- Influence the next generation safeguards and security specialists

The Nature of Security

"The search for static security—in the law and elsewhere—is misguided. The fact is security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts."

-William Osler

Physical Protection System Terminology

- **<u>Safety</u> refers to the systems that react to/in abnormal events by minimizing their impact, preserving human life, and protecting property**

  Event examples: fire, flood, earthquake, natural or human accidents, and earthquakes

- **<u>Security</u> represents the systems that prevent, detect, delay, respond to, interrupt, and neutralize a malevolent human adversary**

  Event examples: industrial espionage, direct facility attack, insider theft, employee strike, and material diversion

Physical Protection System Terminology (continued)

- <u>Safeguards</u> is an integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of SNM
- <u>Operations</u> seeks to produce, transfer, experiment with, store, and maintain products, materials, and work-in-process
  - This implies open access, non-intrusive controls, and limited accountability with the objective of reducing overall costs

MPC&A Physical Protection System
Integration Objectives

- Integrated system of activities, systems, programs, facilities, and policies for the protection of classified information/matter, unclassified controlled information, NMs, weapons, weapon components, property, and equipment
- All contract/subcontract activities included
- Security – the layered “wrapper” or “envelope” around asset(s)
- Protection/Defense-in-depth
- Balanced protection
- Minimized consequence of component failure

Regarding Deterrence …

- Theft, sabotage, and other malevolent acts may be prevented by deterring or defeating an adversary
- Deterrence occurs by implementing measures perceived as being too difficult to defeat:
  - We want to make the target seem "unattractive"
  - Adversary perceives low chance of success and moves to easier target
    - That is, "costs" to attack seem high enough that "payoff" for successful attack are marginal

Regarding Deterrence … (continued)

- The deterrence value of an effective security system may be quite high. That stated, be aware:
  - A visible security system may help discourage certain adversary types. Unfortunately, a determined adversary may choose to attack anyway
  - A motivated and skilled adversary will attack when chances for success are optimized, that is, when facility/target is most vulnerable (night, bad weather, shift change, etc)
  - An adversary may attack based on insufficient or even extensive information on your system. It is difficult to measure how much knowledge an adversary has

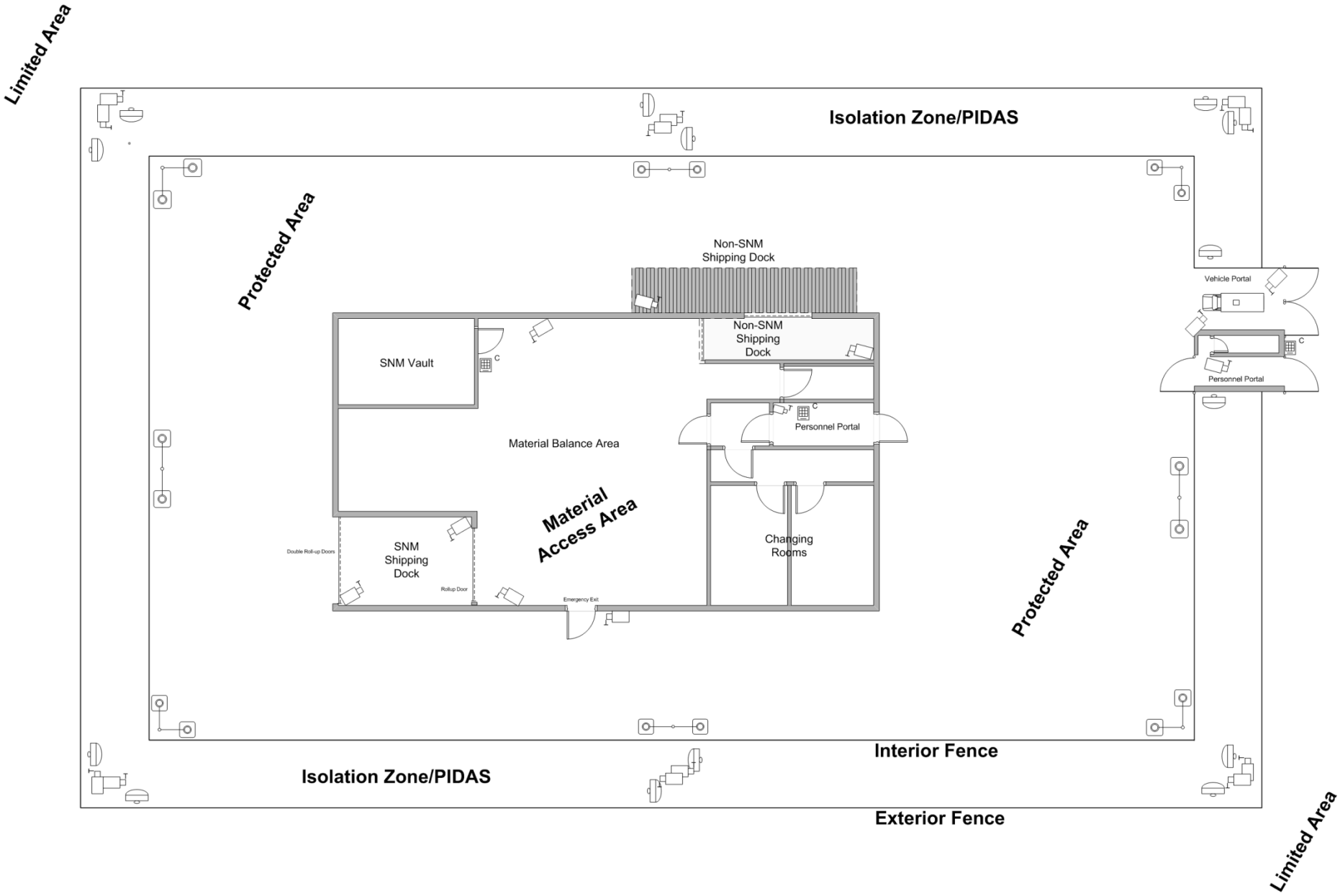
- In each case, deterrence value is negligible!

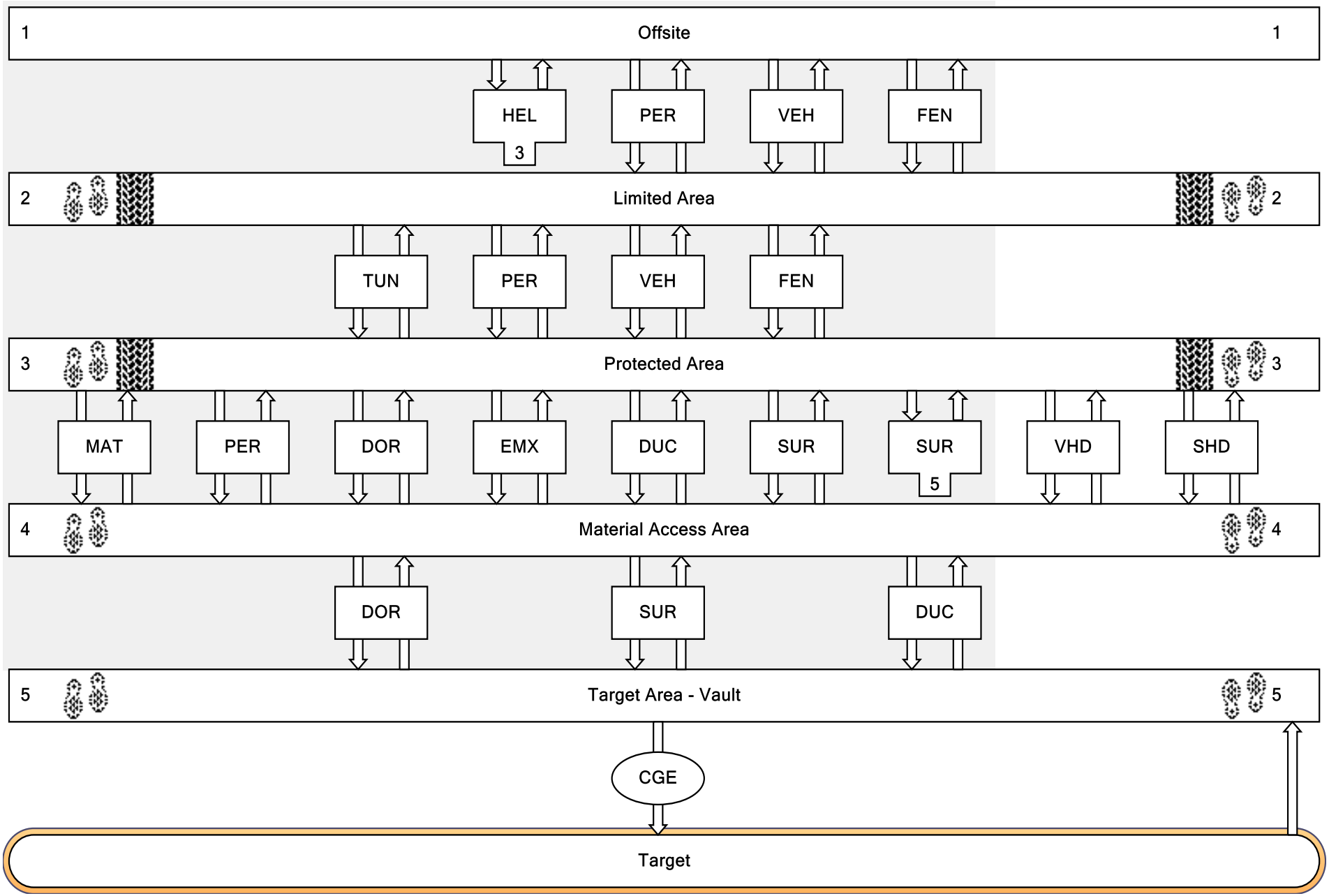
Regarding Deterrence … (continued)

- Do not assume that because the system has not endured an attack that it is an effective system or an effective deterrent
- Deterrence is difficult to measure (based on perception)
- Reliance on deterrence alone is risky; no definitive research exists on deterrent values
- One study shows that deterrent value of a system is actually lower than designers had hoped (Sivarajasingam and Sheperd, 1999)

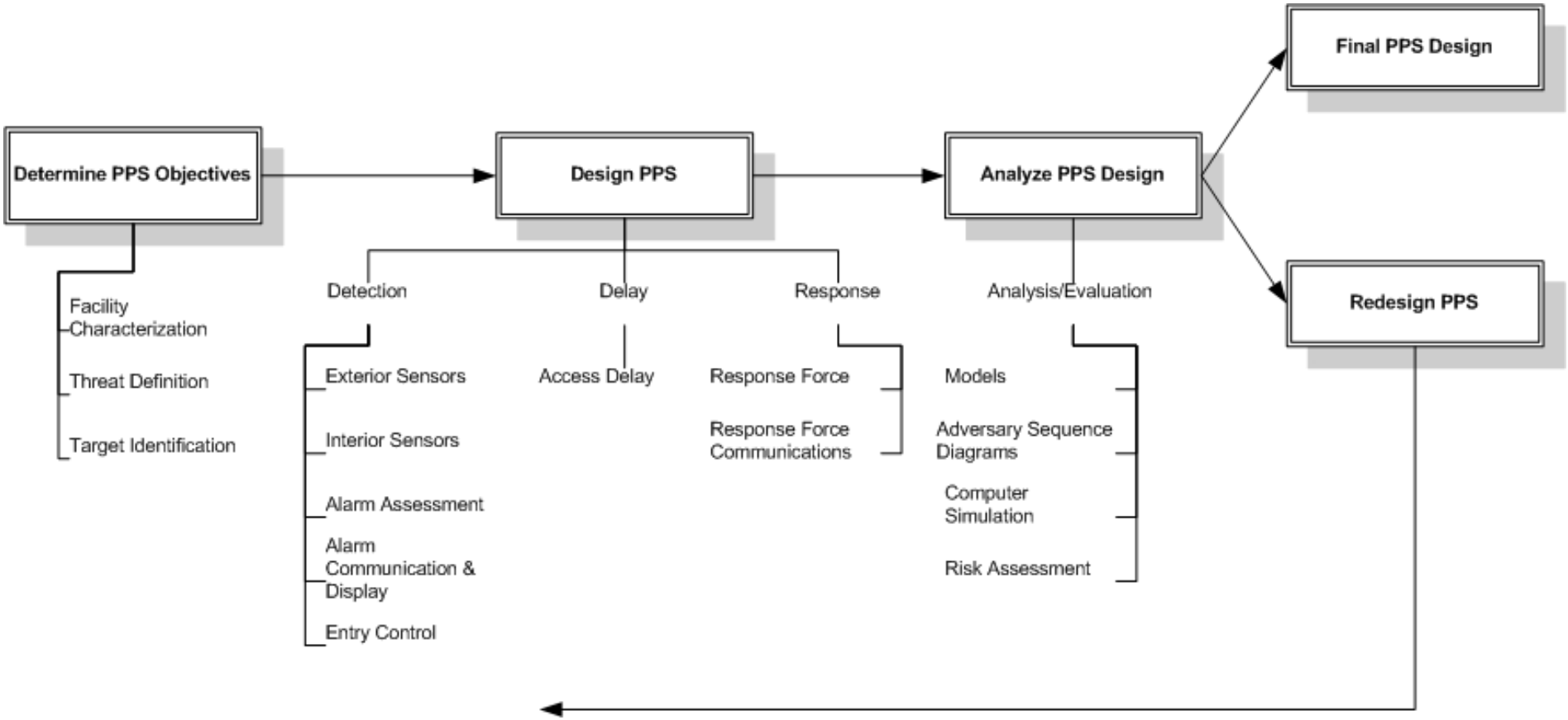
"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

— Bruce Schneier


Limited Area
Isolation Zone/PIDAS
Protected Area
Non-SNM
Shipping Dock
Vehicle Portal
Non-SNM
Shipping
Dock
SNM Vault
C
Personnel Portal
Material Balance Area
Material
Access Area
Changing
Rooms
Double Roll-up Doors
SNM
Shipping
Dock
Rollup Door
Emergency Exit
Protected Area
Interior Fence
Isolation Zone/PIDAS
Exterior Fence
Limited Area


1
Offsite
1
HEL
3
PER
VEH
FEN
2
Limited Area
2
TUN
PER
VEH
FEN
3
Protected Area
3
MAT
PER
DOR
EMX
DUC
SUR
SUR
5
VHD
SHD
4
Material Access Area
4
DOR
SUR
DUC
5
Target Area - Vault
5
CGE
Target

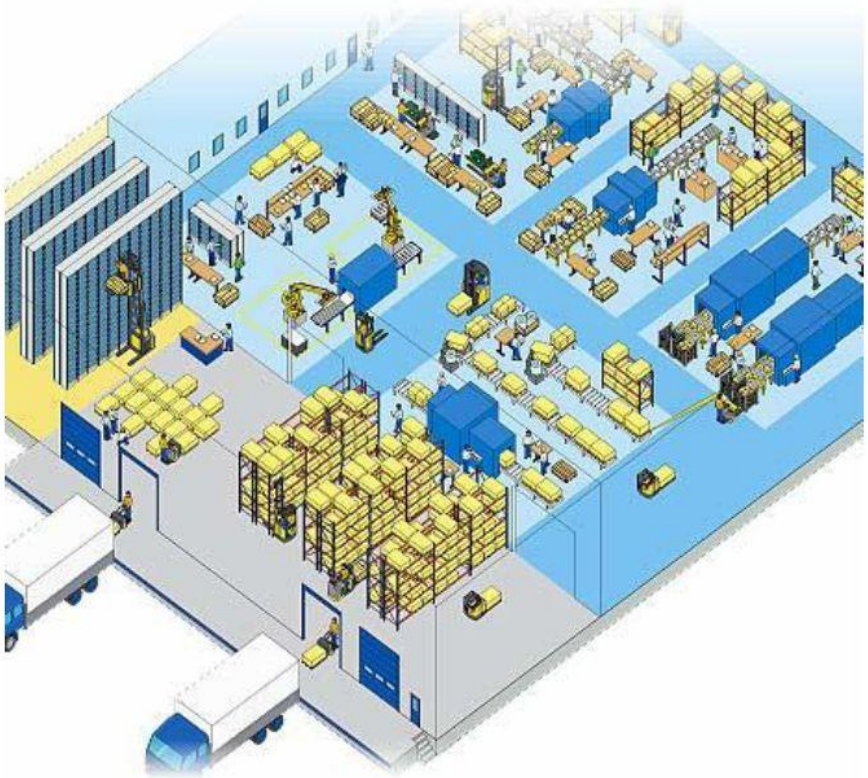
Design and Evaluation Process



Garcia, 2007

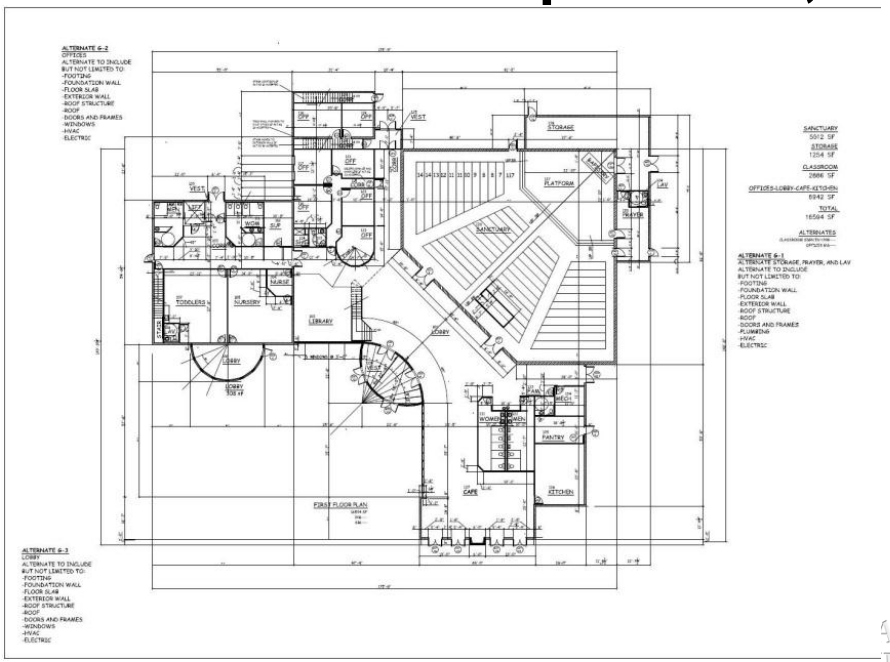
Facility Characterization

- Physical conditions
- Facility operations
- Policies and procedures
- Regulatory requirements
- Safety considerations
- Legal issues
- Corporate goals



Facility Characterization (continued)
Physical Condition

- Easiest area to characterize because much is known and info readily available
- Site boundaries, access points, geography, number of buildings, infrastructure, vegetation, wildlife, climate, existing systems, response forces and their capabilities, and more included …



Facility Characterization (continued)
Facility Operations

- Products of the facility
- Facility processes
- Operating conditions
- Types and numbers of employees
- Review of the operating procedures (usually most time intensive portion of review)
- Operational review of procurement, computing, maintenance, asset tracking, shipping and receiving, workflow, shift changes, accounting functions, vehicle activity

Facility Characterization (continued)
Policies and Procedures

- Many employees use undocumented or unsanctioned work processes
- Right-to-privacy clauses: absolutely essential employees have no expectation of privacy
- No drugs, alcohol, weapons on site
- Use of force by guards
- Clear chain-of-command and responsibilities
- Training, initial and refresher

Facility Characterization (continued)
Regulatory Requirements

- Occupational Safety and Health Administration
- National Fire Protection Association
- Department of Labor
- Environmental Protection Agency
- Underwriter's Laboratory
- Department of Energy Orders, Rules, and/or Regulations
- Local commissions:
  - Safety and security-related aspects of a facility cannot violate federal regulations.

Facility Characterization (continued)
Safety Considerations

- Safety and safeguards and security do not have the same goals.
- Example: fire evacuation

- Integration of systems may not be completely possible, but they should be complementary in purpose by:
  - providing protection of assets; and
  - decreasing risks for injury or death.

Facility Characterization (continued)
Legislation

- Most complex in implementing a system; legislation covers:
  - liability;
  - privacy;
  - disabled access;
  - labor relations;
  - employment practices;
  - guard and nuclear material training;
  - failure to protect; and
  - excessive use of force (overreaction).
- Knowledge of the criminal justice system is important!

Facility Characterization (continued)
Corporate Goals

- View of security by corporate officials:
  - Required but expensive, provides no value, not a producer

    or
  - Absolutely essential, protects vital assets and people, reduces risk and liability
- Corporate decisions and events that impact security:
  - Economy (layoffs)
  - Labor disputes
  - Facility or product expansion or shrinkage
  - Executive/Dignitary visits
  - New products/procedures

Threat Definition

- **Steps for threat definition:**
  - **List information needed to define threat:**
    - **Who:**
      - **Outsiders**
      - **Insiders**
      - **Outsiders working in collusion with insiders**
    - **Why (motivation):**
      - **Ideological**
      - **Economic**
      - **Personal**
      - **Pathological**

"Water shapes its course according to the nature of the ground over which it flows; the soldier works out his victory in relation to the foe whom he is facing."

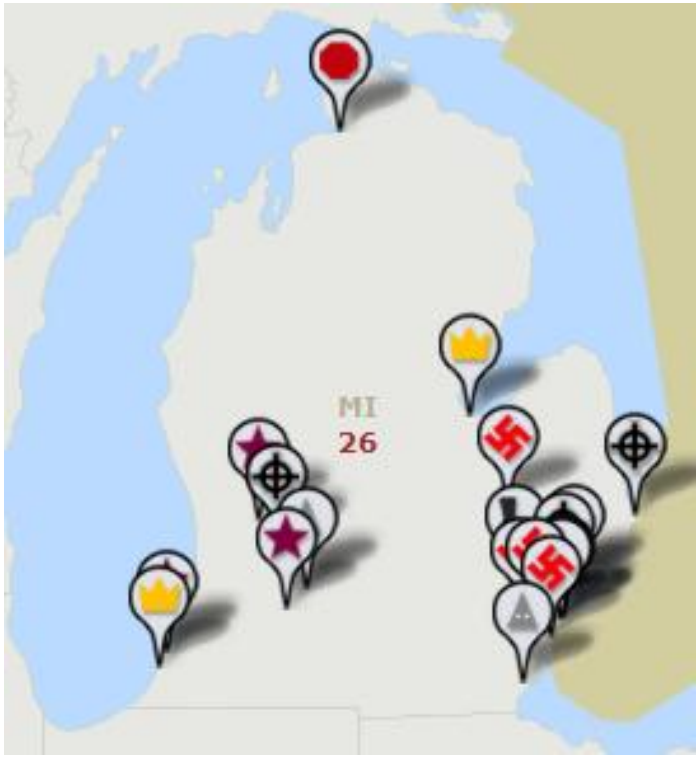
-Sun Tzu, *The Art of War*, 6th Century B.C.

Threat Definition (continued)

- Base potential goals on targets assuming:
  - How (tactics):
    - Force
    - Stealth
    - Deceit (includes use by insiders)
  - Numbers and capabilities:
    - Vehicles, tools, resourcefulness, system knowledge
- Collect information on potential threat:
  - Intelligence sources (DoD, DOS, DHS, DOE; usually classified)
  - Crime analysis (FBI, Secret Service NTAC; sensitive or OUO)
  - Professional organizations (ASIS, InfraGard)
  - Published literature
  - Government directives (usually reactive, not proactive)

Threat Definition (continued)

Name	Type	City
American Nazi Party	Neo-Nazi	Westland
By Yahweh's Design	Christian Identity	Stevensville
Charles Darwin Research Institute	White Nationalist	Port Huron
Council of Conservative Citizens	White Nationalist	Caledonia
Firm 22	Racist Skinhead	
Jewish Defense League	General Hate	
Nation of Islam	Black Separatist	Detroit
Nation of Islam	Black Separatist	Grand Rapids
Nation of Islam	Black Separatist	Highland Park
Nation of Islam	Black Separatist	Benton Harbor
National Knights of the Ku Klux Klan	Ku Klux Klan	Dowling
National Socialist Aryan Order	Neo-Nazi	Davison
National Socialist Movement	Neo-Nazi	Detroit
New Black Panther Party	Black Separatist	
Northern Hammerskins	Racist Skinhead	Detroit
NS Publications	Neo-Nazi	Wyandotte
Romanian National Vanguard	Neo-Nazi	
Social Contract Press	Anti-Immigrant	Petoskey
United Northern and Southern Knights of the Ku Klux Klan	Ku Klux Klan	Fraser
United White Knights of the Ku Klux Klan	Ku Klux Klan	Detroit
United White Knights of the Ku Klux Klan	Ku Klux Klan	Monroe
United White Knights of the Ku Klux Klan	Ku Klux Klan	
Vinlanders	Racist Skinhead	
Volksfront	Racist Skinhead	Detroit
Vox Nationale	White Nationalist	Warren
Yahweh's Truth	Christian Identity	Essexville



Source: SPLC.org

Threat Definition (continued)

- Then organize it into usable information:
  - Outsider adversary threat spectrum
  - Sample threat statements
  - Design Basis Threat (DBT)
- Perform target identification:
  - Manual listing
  - Sabotage fault trees and fault tree analysis (FTA)
  - Consequence analysis

"We only need to be lucky once. You need to be lucky every time."

--The IRA to Margaret Thatcher, after a failed assassination attempt

Target Identification

- Manual listing:
  - Works best for small areas
  - Manageable lists of equipment
  - Simple processes
- Consequence analysis:
  - Prioritization of assets (targets) based on consequence of loss:
    - (1) List targets
    - (2) Determine consequence of loss
    - (3) Estimate probability of loss
  - Can measure in dollars, loss of life, loss of reputation, etc.

Target Identification (continued)

	Low Probability	Medium Probability	High Probability
High Consequence	Direct Attack (Terrorist)		
Medium Consequence		Sabotage (Insider)	
Low Consequence			Graffiti (Vandals)

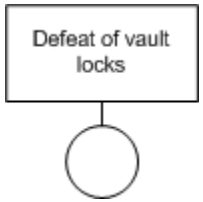
The general who wins a battle makes many calculations before the battle is fought. Many calculations lead to victory and few calculations to defeat.

Sun Tzu, *The Art of War*, 6th Century B.C.

Target Identification (continued)

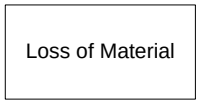
- **Fault Tree Analysis (FTA):**

Basic event, this is the beginning



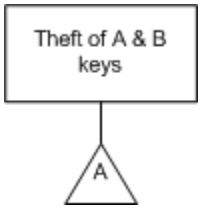
"And" gate: all listed events must occur to pass this gate

Supporting event or final event



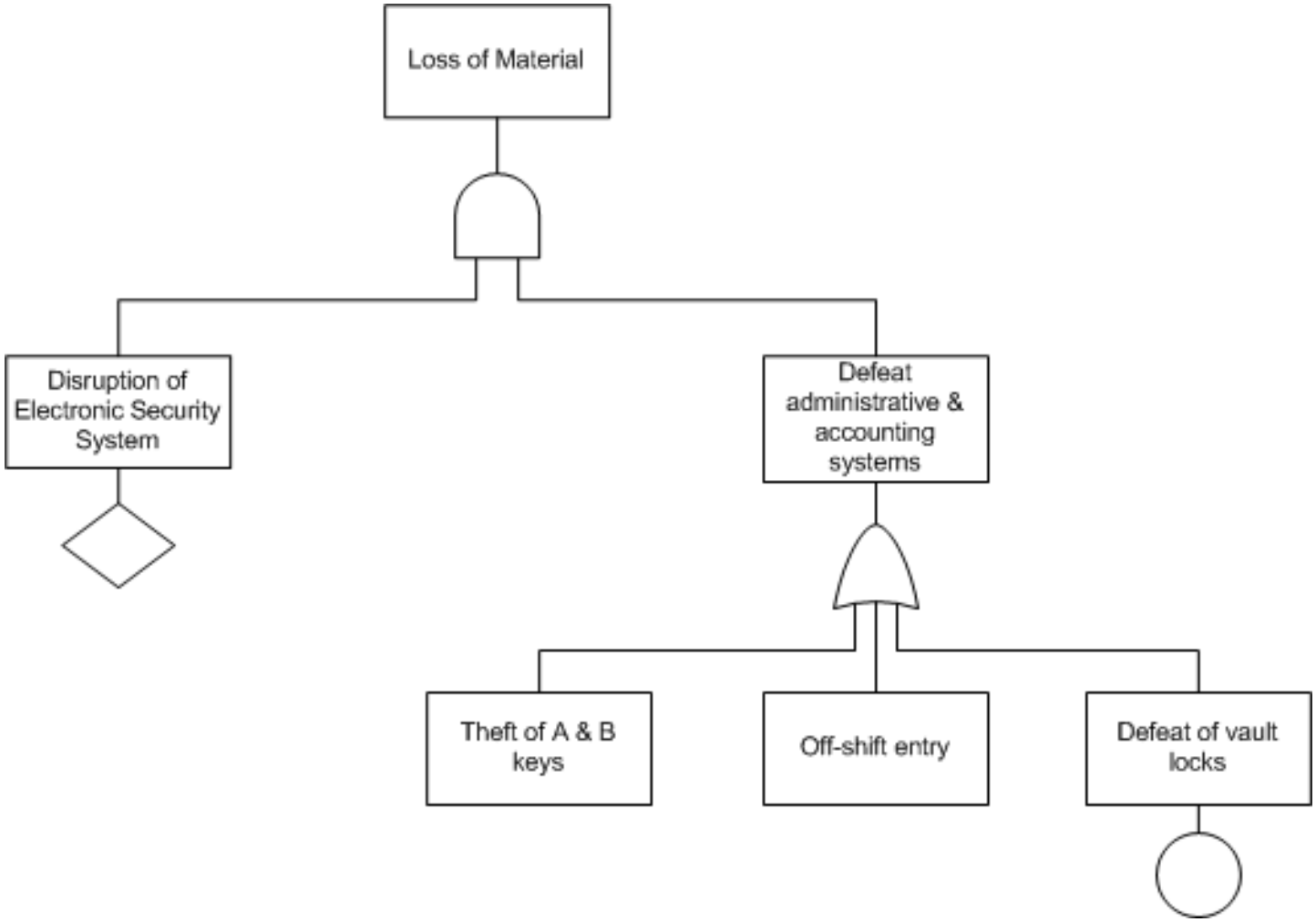
"Or" gate: any listed events can occur to pass this gate

Undeveloped Event



Continued event from chart "A"

Target Identification (continued)



Vulnerabilities vs Threats

- **Threats surveys and vulnerability assessments can proceed in parallel, but eventually must be correlated.**

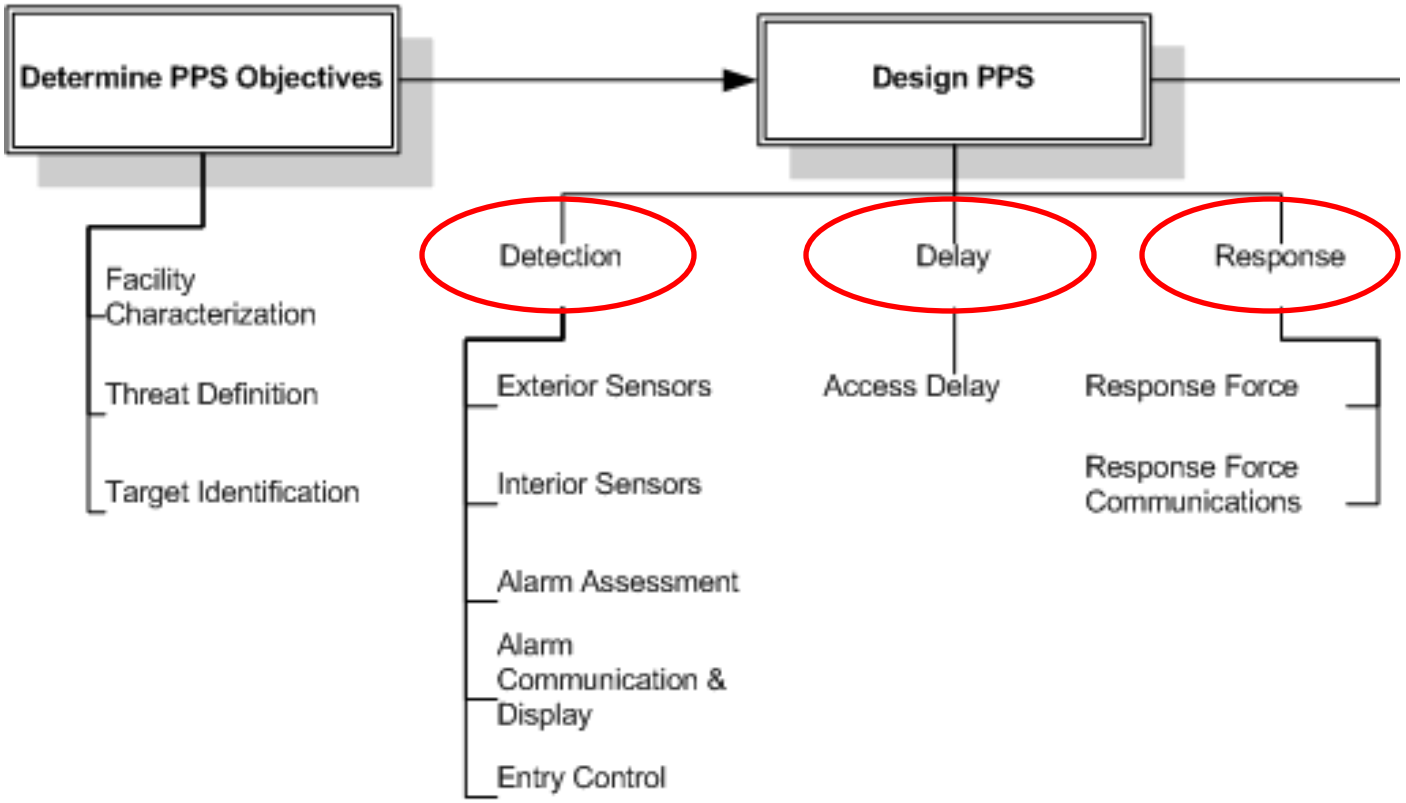
<u>Vulnerabilities Trump Threats Maxim:</u>

"If you know the vulnerabilities (weaknesses), you've got a shot at understanding the threats (the probability that the weaknesses will be exploited, how, and by whom)."

-Roger Johnston, ANL

Three Critical Factors for Security Design

- Detection
- Delay
- Response



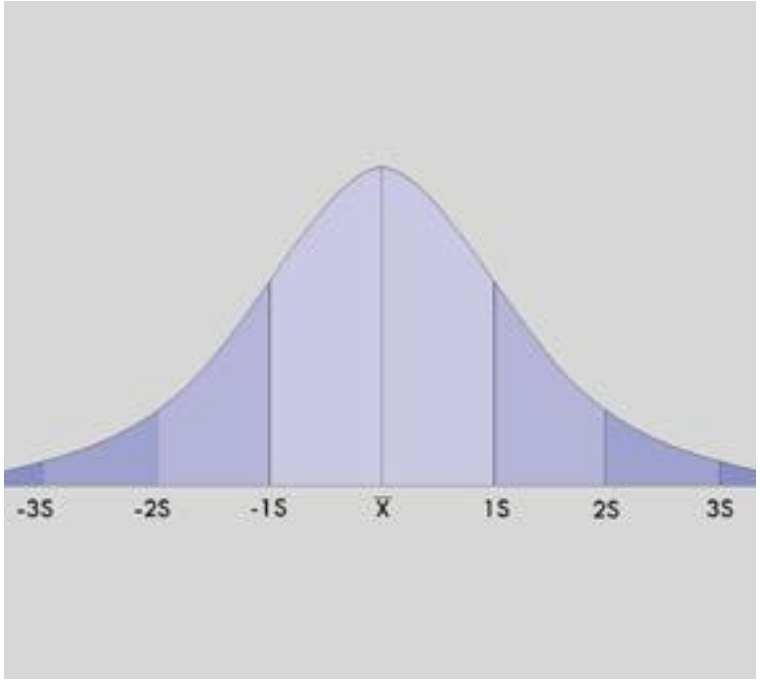
Garcia, 2007

Detection

- **What is detection?**
- **Which systems are involved?**
- **When is an adversary or malevolent action considered "detected?"**

<u>Detection without assessment *is not* detection</u>.

Detection (continued)
Sensor Classification



- P_D (probability of detection)
  - @ given C_L (confidence level)
  - Ex: .95 P_D * .95 C_L = .903 or 90%
  - Problem: C_L is undefined
  - Sensor "target" varies
  - Sensor "phenomenology" environmentally dependent
  - Expect about 90% or .90 P_D (or lower if skilled adversary)
- NAR (nuisance alarm rate; false alarm is a type of nuisance alarm)
- Vulnerability to defeat (seconds/probability to defeat)
  - Spoof, bypass, or direct attack

Detection (continued)
Sensor Classification

Interior Intrusion Sensors

- Electro-mechanical
- Active Infrared
- Vibration
- Capacitance
- Fiber-optic
- Microwave
- Ultrasonic
- Sonic
- Passive infrared
- Proximity sensors
- Pressure

Exterior Intrusion Sensors

- Electro-mechanical
- Seismic pressure
- Magnetic field
- Ported coaxial cable
- Fiber-optic cable
- Electric field
- Active infrared
- Passive infrared
- Microwave
- Dual technology
- Video motion detection
- Radar/laser

Red: Most commonly deployed

Detection (continued)
Assessment

- **Alarm assessment:**
  - Assessment versus surveillance
  - Detection → Classification → Identification
  - Camera, lens (focal length, resolution, frames per second, f-number, distance and width)
  - Lighting (lumens, surface reflectivity, uniformity, heat/color, and air clarity)
  - Transmission (concentration, encryption, compression)

Detection (continued)
Assessment

- Alarm Communication and Display (AC&D):
  - Components:
    - Servers (processing, storage, and retrieval), network hardware, workstation computers, printers, monitors, keyboard, mouse, uninterruptible power supply (UPS)
  - Ergonomics
  - Operator overload
  - Operator effectiveness
    - Human factors engineering

Detection (continued)
Entry Control

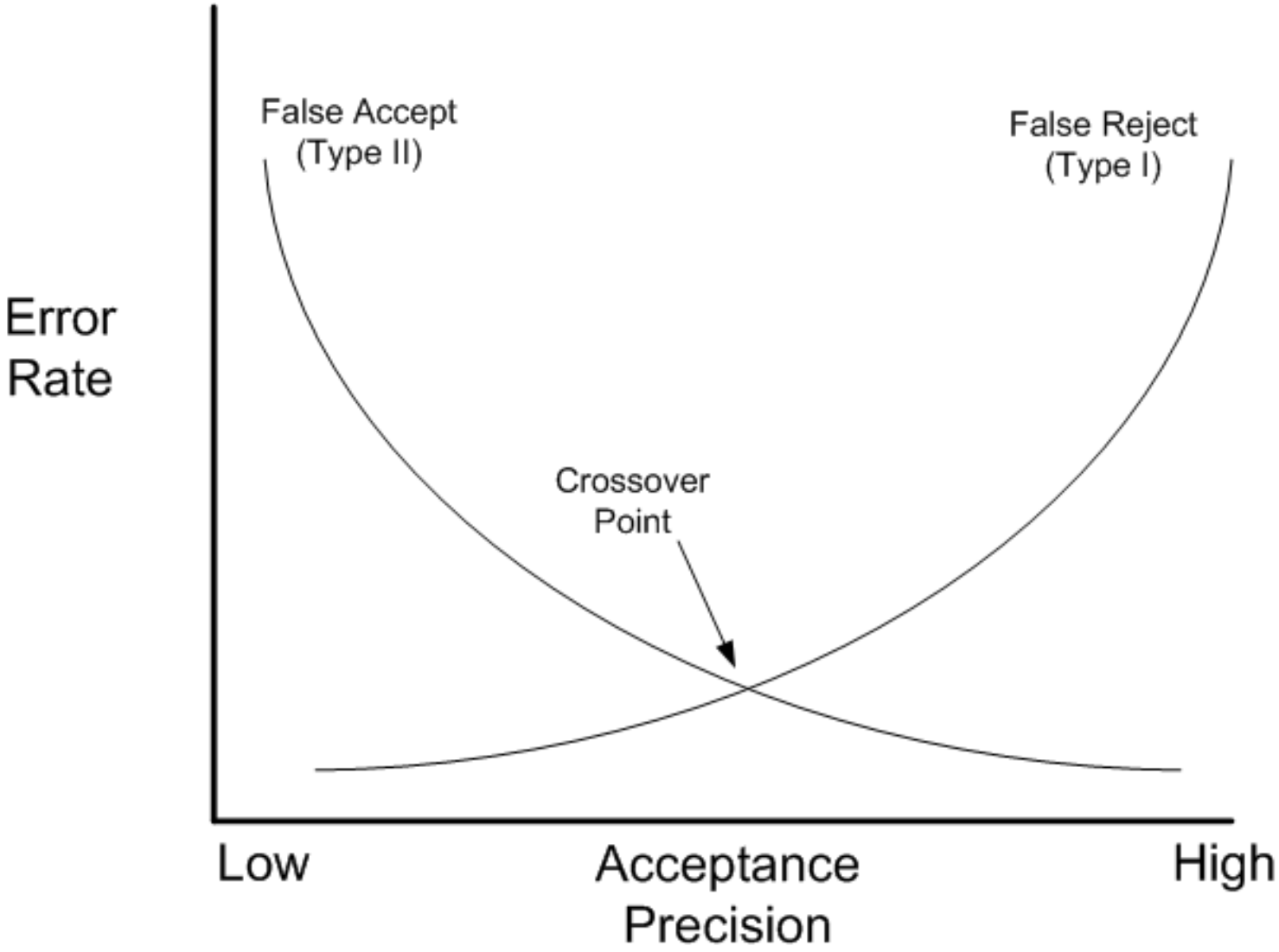
"Badges? We ain't got no badges! We don't need no badges. I don't have to show you any stinkin' badges!"

— from the film *Treasure of Sierra Madre*

Detection (continued)
Entry Control

- Entry control versus access control
- PINs (personal identification numbers)
- Credentials:
  - Photo ID (identification), exchange badge, stored-info badge, and coded credential
- Identity verification (biometrics)
- Measures (and balances) Type I & II errors (false reject and false accept)
- Problem: Most entry control systems are not monitored for spoof or Type I or II errors, just tamper. Worse, they balance Type I and Type II errors

Detection (continued)
Entry Control



Delay

"If the enemy leaves a door open, you must rush in. All we need do is to throw something odd and unaccountable in his way."

-Sun Tzu, *The Art of War*, 6th Century B.C.

Delay (continued)

- Delay (measured in seconds)
- Access delay:
  - Fences
  - Gates
  - Vehicle barriers
  - Structural barriers:
    - Walls and doors
    - Windows and utility ports
    - Roofs and floors
  - Dispensable barriers

Delay before detection is primarily a deterrent.

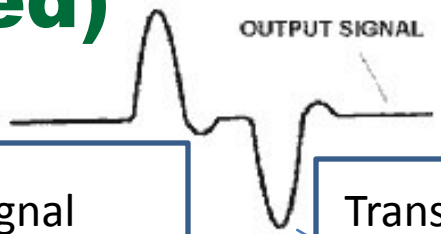
Delay (continued)

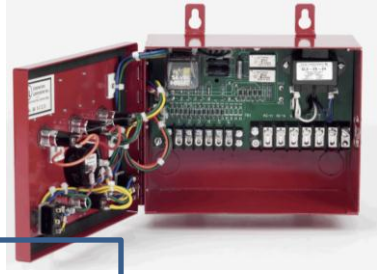
- What are dispensables?
  - Sticky foam, for example…

Wired.com image

Defensetech.com image

Detection (continued)
Sensor Classification





On-board processing to measure and chronograph signal

Alarm signal generated

Transmitted to alarm concentrator

Concentrator relays signal to Central Alarm System

Central Alarm System prioritizes/displays alarm, captures assessment video, and presents playback to operator

Operator accepts and assesses alarm

Nuisance alarm?

Y

Operator dispositions alarm

N

Operator dispatches response

Delay

- Access delay:
  - Fences
  - Gates
  - Vehicle barriers
  - Structural barriers:
    - Walls and doors
    - Windows and utility ports
    - Roofs and floors
  - Dispensable barriers

Delay before detection is primarily a deterrent.

Safeguards Integration with Physical Protection System

- <u>Security</u> represents the systems that prevent, detect, delay, respond to, interrupt, and neutralize a malevolent human adversary.
- <u>Safeguards</u> is an integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of NM.

Safeguards Integration with Physical Protection System (continued)

- Operations (usually manufacturing) seeks to produce, transfer, experiment with, store, and maintain.
  - This implies open access, non-intrusive controls, and limited accountability with the objective of reducing overall costs.
- MBA (Material Balance Area) Custodian is an individual assigned responsibility for the control of NM in a localized area of a facility (a single MBA).

Safeguards Integration with Physical Protection System (continued)

- **<u>Material Control and Accountability (MC&A)</u> are the parts of the safeguards program designed to provide information on control and assurance of the presence of NMs including those systems necessary to establish and track NM inventories; control assess to; detect loss or diversion of NM; ensure the integrity of NM; and ensure the integrity of those systems and measures.**

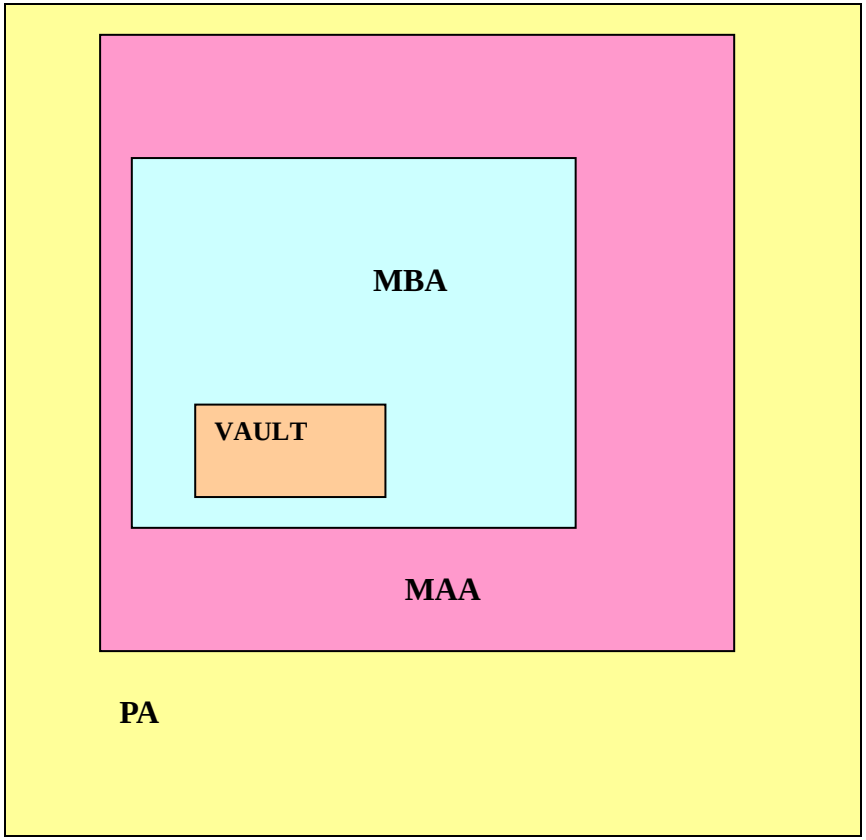
Safeguards Integration with Physical Protection System (continued)

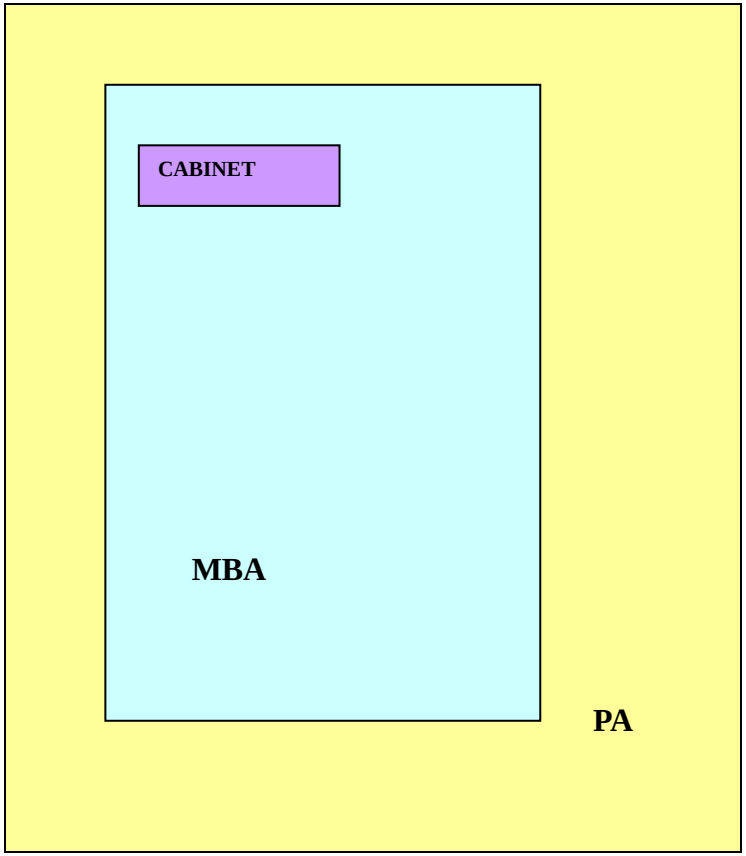
- **Protected Area (PA)** is a type of security area defined by physical barriers (i.e., walls or fences) and surrounded by intrusion detection and assessment systems to which access is controlled.
- **Material Access Area (MAA)** is a type of security area approved for use, process, and/or storage of a Category I quantity of special nuclear material (SNM) that has specifically defined physical barriers, is located within a protected area, and is subject to specific access controls.

Safeguards Integration with Physical Protection System (continued)

- <u>Material Balance Area (MBA)</u> is an area that is both a subsidiary account of material at a facility and a single geographical area with defined boundaries and is an integral operation used to identify the location and quantity of NMs in the facility.
- <u>Vaults, Vault Type Rooms, and Cages</u> are enclosures, usually equipped with intrusion detection systems, used for storing material.

Physical Layers of Protection





Characteristics of Effective MPC&A Design

- Effective organization
- Audits/Assessments frequently/thoroughly:
  - Safeguards 1st principle initiative
- Human Reliability Programs (HRP)
- Effective physical control
- Effective material surveillance
- Effective accounting systems
- Effective measurement systems

MPC&A Components

- **Program Administration**
- **Material Accounting**
- **Material Control**

Program Administration

- Program elements:
  - Drivers:
    - Regulations, manuals, orders, procedures
  - Graded safeguards:
    - Level of control and accountability graded based on consequence of loss
    - Greatest amount of control and accountability for types and quantities of SNM most easily used to initiate a nuclear reaction
  - Performance testing/requirements:
    - MC&A procedures and practices verification; demonstration of material controls effectiveness; access controls, material surveillance, tamper indicating devices (TIDs), accounting systems, measurements, etc.
    - Performance tests based on graded safeguards approach

Program Administration (continued)

- Training:
  - Individuals responsible for performing MPC&A-related functions must possess sufficient knowledge to perform tasks in acceptable approved manner
  - Requirements, systems, and technologies
  - Physical inventories, measurements, transfers
  - State system of accounting and control
  - Export controls

Material Accounting

- **Measurements/measurement control:**
  - **Must be precise and sufficiently accurate to minimize the contribution of measurement error to limit the error of the inventory difference**
  - **Should be independent of the operations**
  - **Should have sampling programs in place to ensure portions of bulk material taken for measurement are representative of the bulk material**

Material Accounting (continued)

- Measurement methods must be established for all NM on inventory:
  - Scales and balances
  - Nondestructive analysis
  - Destructive analysis
  - Holdup measurements
- Documented notification and responses are required if NM has been removed or other abnormal situation is detected.
- Information is entered into the accounting system.

Material Accounting (continued)

- Transfers:
  - External transfers:
    - Communication between shipper and receiver prior to shipment
    - Immediately after receipt, transfer check completed:
      - Transfer checks consist of confirmation of the shipping container or item count, validation of the TID, and comparison of shipping documentation to ensure shipment was received intact.
    - Receiver confirmation and verification/accountability measurements based on graded safeguards approach
    - Discrepancies must be reconciled between shipper/receiver
    - Transaction information entered into accounting system

Material Accounting (continued)

- **Transfers:**
  - **Internal transfers:**
    - **Communication between shipper and receiver prior to shipment**
    - **Material subject to transfer check:**
      - **Transfer checks consist of confirmation of the shipping container or item count, validation of the TID, and comparison of shipping documentation to ensure shipment was received intact.**
    - **Material should have measured value and confirmation/verification completed at receipt**
    - **Acceptance/rejection criteria established to evaluate measurement data**
    - **Documented notification and responses if NM has been removed or other abnormal situation detected**
    - **Transaction information entered into the accounting system**

Materials Accounting (continued)

- Non-SNM transfers (MPC&A):
  - Preliminary measurement (monitoring)
  - Material must be monitored immediately prior to removal from facility to ensure no NM/SNM present
  - Any abnormalities resolved prior to removal of material from the Material Access Area (MAA)

Materials Accounting (continued)

- Accounting:
  - Accounting system:
    - A complete audit trail for all NM from receipt to disposition:
      - Track NM inventories, document NM transactions
  - Physical inventories:
    - Actual materials verified in their stated quantities; detection of unauthorized removal of NM
    - Items with measured values
    - Frequency based on graded safeguards approach
    - Special inventories
    - Inventory verification/confirmation
    - Reconciliation (physical inventory comparison to book inventory):
      - Resolve any discrepancies

Materials Accounting (continued)

- Process monitoring is dividing an MBA or processing area into process units to identify process anomalies outside of normal process variation (i.e., determining the appropriate losses/gains surrounding a process).
- Acceptable Losses are losses that are within the identified range for a particular process/activity.

Material Control

- Material control:
  - Access controls:
    - The graded safeguards approach must be utilized.
    - Only authorized personnel have access to NM.
    - Only authorized personnel have access to the MPC&A data, information, measurement equipment, and accountability system.
  - Material surveillance:
    - The graded safeguards approach must be utilized.
    - This includes automated systems including monitoring devices, sensors, and visual surveillance/direct observation such as a "two-person rule":
      - The two-person rule stipulates that the observer must have the means to recognize, assess, and report unauthorized activities.

Material Control (continued)

Graded Safeguards

	Attractiveness Level	Pu/U-233 Category (kg)				Contained U-235/Separated Np-237/ Separated Am-241 and -243 Category (kg)				All E Materials Category IV
		I	II	III	IV[1]	I	II	III	IV[1]	
WEAPONS Assembled weapons and test devices	A	All	N/A	N/A	N/A	All	N/A	N/A	N/A	N/A
PURE PRODUCTS Pits, major components, button ingots, recastable metal, directly convertible materials	B	≥2	≥0.4 <2	≥0.2 <0.4	<0.2	≥5	≥1 <5	≥ 0.4 <1	<0.4	N/A
HIGH-GRADE MATERIALS Carbides, oxides, nitrates, solutions (≥25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; UF_4 or UF_6 (≥ 50% enriched)	C	≥6	≥2 <6	≥0.4 <2	<0.4	≥20	≥ 6 <20	≥2 <6	<2	N/A
LOW-GRADE MATERIALS Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; moderately irradiated material; Pu-238 (except waste); UF_4 or UF_6 (≥20% <50% enriched)	D	N/A	≥16	≥3 <16	<3	N/A	≥50	≥8 <50	<8	N/A
ALL OTHER MATERIALS Highly irradiated forms, solutions (<1 g/L), uranium containing <20% U-235 or <10% U-233[2] (any form, any quantity)	E	N/A	N/A	N/A	Reportable quantities	N/A	N/A	N/A	Reportable quantities	Reportable quantities

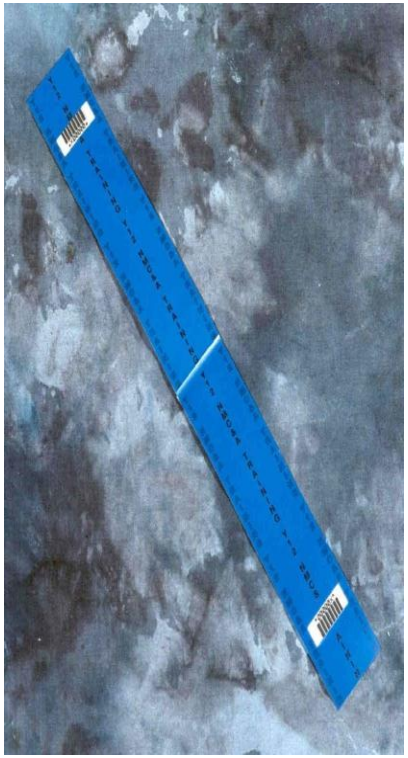
Material Control (continued)

- Material containment:
  - Program in place to provide controls for NM operations relative to MAAs, Protection Areas (PAs), MBAs
  - Utilize the graded safeguards approach:
    - Material can only be stored/processed within an MBA contained within an MAA contained in a PA
    - Material can only be stored/processed within an MBA contained in a PA
    - Material can be stored in an MBA
  - Controls established for NM being used or stored in processing areas:
    - Activities and locations for storing material, response actions in abnormal situations

Material Control (continued)

- Detection assessment:
  - Detect and assess unauthorized removal of NM using graded safeguards approach
  - Interface with facility's physical protection system:
    - Detect and localize removal of material from an authorized location and notify protective force when such events are detected
  - Tamper Indicating Devices (TIDs):
    - Control TIDs through a documented program (TIDs detect violations of container integrity)
  - Portal monitoring:
    - Base Detection Level on types and forms of SNM used, stored, or processed – graded safeguards approach

Material Control (continued)
TID Examples



Material Control (continued)

- **Waste monitors:**
  - **Liquid, solid, and gaseous waste streams leaving an MAA must be monitored to detect theft or diversion of SNM.**
- **Daily administrative checks:**
  - **A daily review will be provided for timely identification of obvious abnormalities or missing items *or* to ascertain that there is no indication of tampering.**

Physical Security Response

The spot where we intend to fight must not be made known. Numerical weakness comes from having to prepare against possible attacks.

Sun Tzu, *The Art of War*, 6th Century B.C.

Physical Security Response

- What is response?
  - What processes precede response?
- When is an adversary interrupted?
- When is an adversary neutralized?

"Hence that general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to attack."

-Sun Tzu, *The Art of War*, 6th Century B.C.

Physical Security Response (continued)

- Inputs to the system effectiveness equation:

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

$$P_E = P_I * P_N$$

$$P_I = P_D * P_{AC} * P_{AD}$$

Where:

P_I = Probability of Interruption (0-1)

P_D = Probability of Detection = $P_S * P_T * P_A$ (0-1)

P_{AC} = Probability of Accurate Communication (0-1)

P_{AD} = Probability of Timely Deployment (0-1)

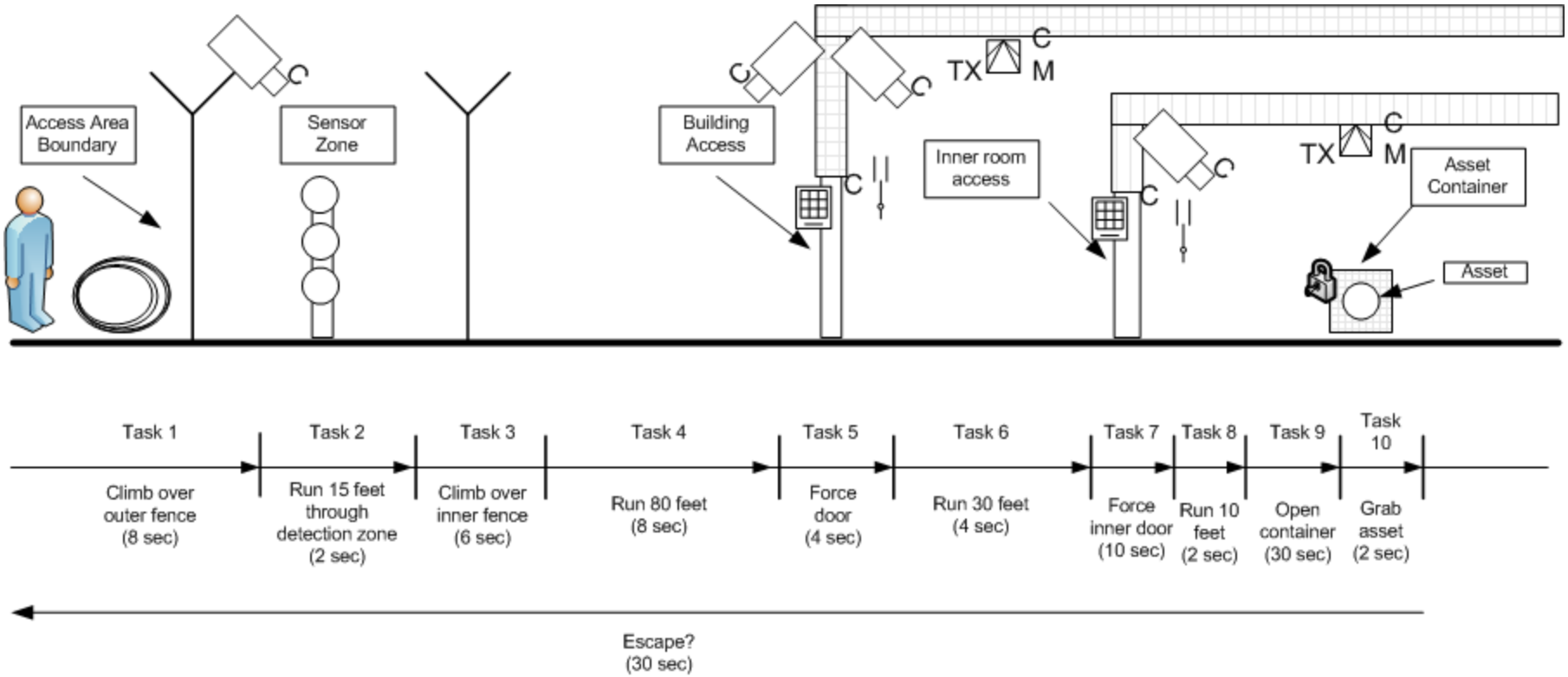
Physical Security Response (continued)

- Response force calculations:
  - Probability of Interruption (P_I)
  - Response Force Time (RFT)
  - Critical Detection Point (CDP)
- Response force communications
- Response force training
- Response force weapons

"If you know the enemy and know yourself, you need not fear the result of a hundred battles....If you know neither the enemy nor yourself, you will succumb in every battle."

-Sun Tzu, *The Art of War*, 6th Century B.C.

Physical Security Response (continued)



MPC&A Responses

- Isolate area of concern
- Determine necessary actions:
  - Need for special inventory
  - Measurements of material in question
- Report status to all parties involved (management, operations personnel, etc.)
- Release area when anomalies resolved

Physical Protection System Evaluation

- Vulnerability assessment
- Performance assessment

MPC&A Evaluation

- Performance test conducted to ensure requirements met in operations area
- Independent assessments conducted to ensure requirements met in operations area and in MPC&A organization
- Self-assessments
- Safeguards First Principle Initiative

Summary

- It is our hope that in the course of this presentation *you* have gained:
  - *insight* into the security and management of nuclear materials;
  - *increased awareness* of these operational activities; and
  - *heightened interest* so that *you* may become the *next generation of safeguards and security specialists*.

Summary (continued)

- Questions and Answers
- Evaluation Form

Academic Attribution/Citations

- National Institute of Security Engineers East, *Perimeter Security Sensor Technologies,* DARPA,1997.
- Barnard. R. L., *Intrusion Detection Systems*, Butterworth, 1988.
- Fischer, R. J., and Green, G., *Introduction to Security*, 7th ed. Butterworth Heinemann, 2005.
- Garcia, M. L., *The Design and Evaluation of Physical Protection Systems*, Butterworth Heinemann, 2007.
- Garcia, M. L., *Vulnerability Assessment of Physical Protection Systems*, Butterworth Heinemann, 2006.
- Sivarajasingam, V., and Sheperd, J. P., *Effect of closed circuit television on urban violence,* Journal of Accident and Emergency Medicine, 1999; 16(4):255-257.