Exceptional service in the national interest

SAND2013-8129P

Sandia National Laboratories

Threat Definition and Characterization

David Ek

Korea Hydro Nuclear Power/Central Research Institute Visit
September 23 – October 4, 2013

U.S. DEPARTMENT OF ENERGY | National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2013-XXXXP

ACKNOWLEDGEMENT: Includes content from SAND2009-1437P , SAND2011-XXXXP, and SAND2012-5719P

Objectives

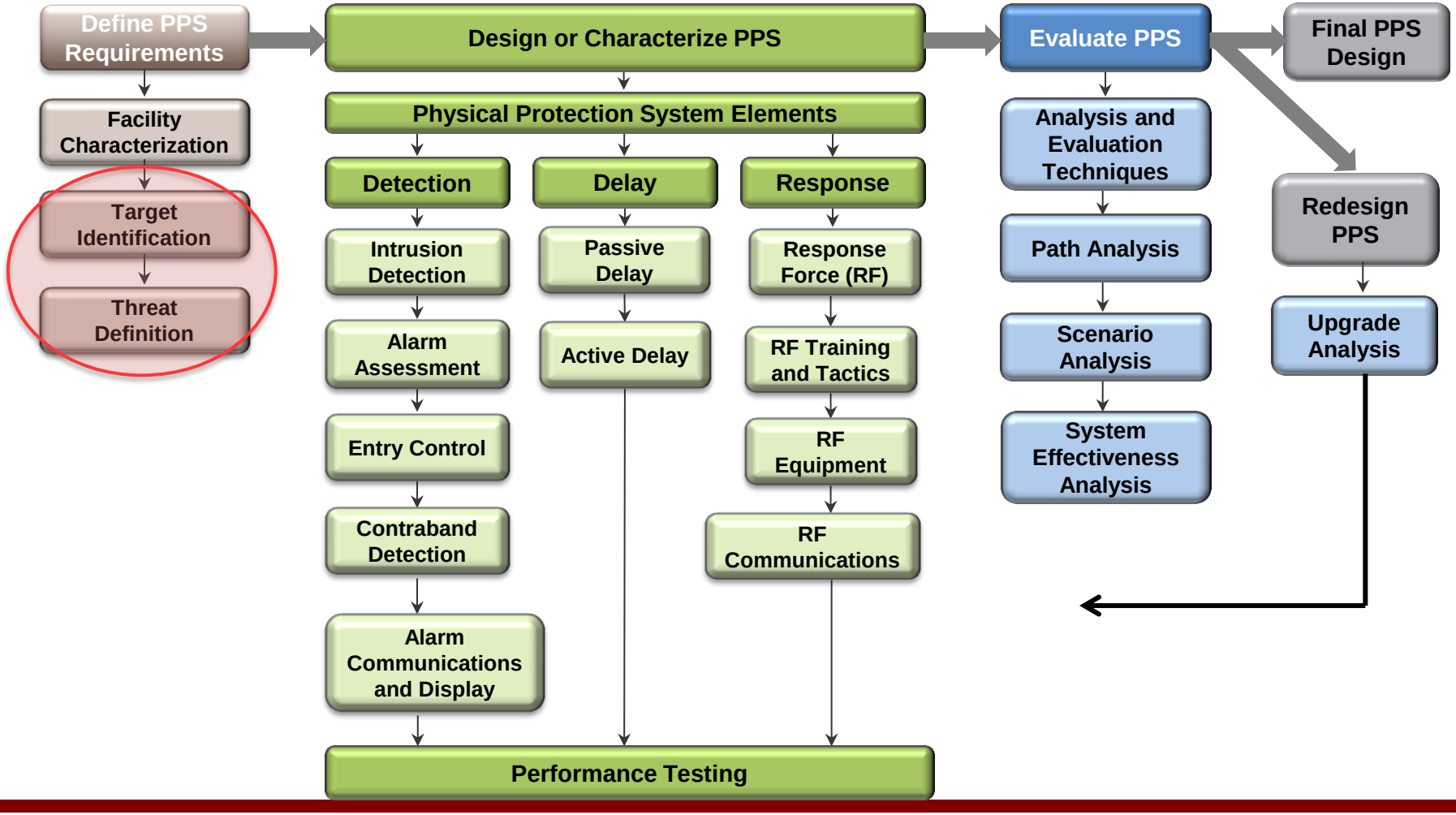
- After this presentation, you should be able to:
  - Identify major targets
    - Be familiar with consequences of concern
  - Develop threat characterization through the process steps
  - Understand threats and development of a Design Basis Threat (DBT)
  - Define adversary types and capabilities
  - Define possible natural hazards and accidents base on an extended analysis process
  - Develop a Threat Spectrum

Outline

- Target Definition
- Threat Definition
- Adversary Definition
- Capability Definition
- Natural Hazards
- Human induced Accidents
- Threat Spectrum

Design Evaluation Process Outline

- Physical Protection System Design and Evaluation



Definitions

- Threat Assessment – An analysis that documents the credible motivations, intentions, and capabilities of potential adversaries that could cause undesirable consequences to nuclear materials and nuclear facilities
  - One of the major inputs for the Design Basis Threat (DBT)

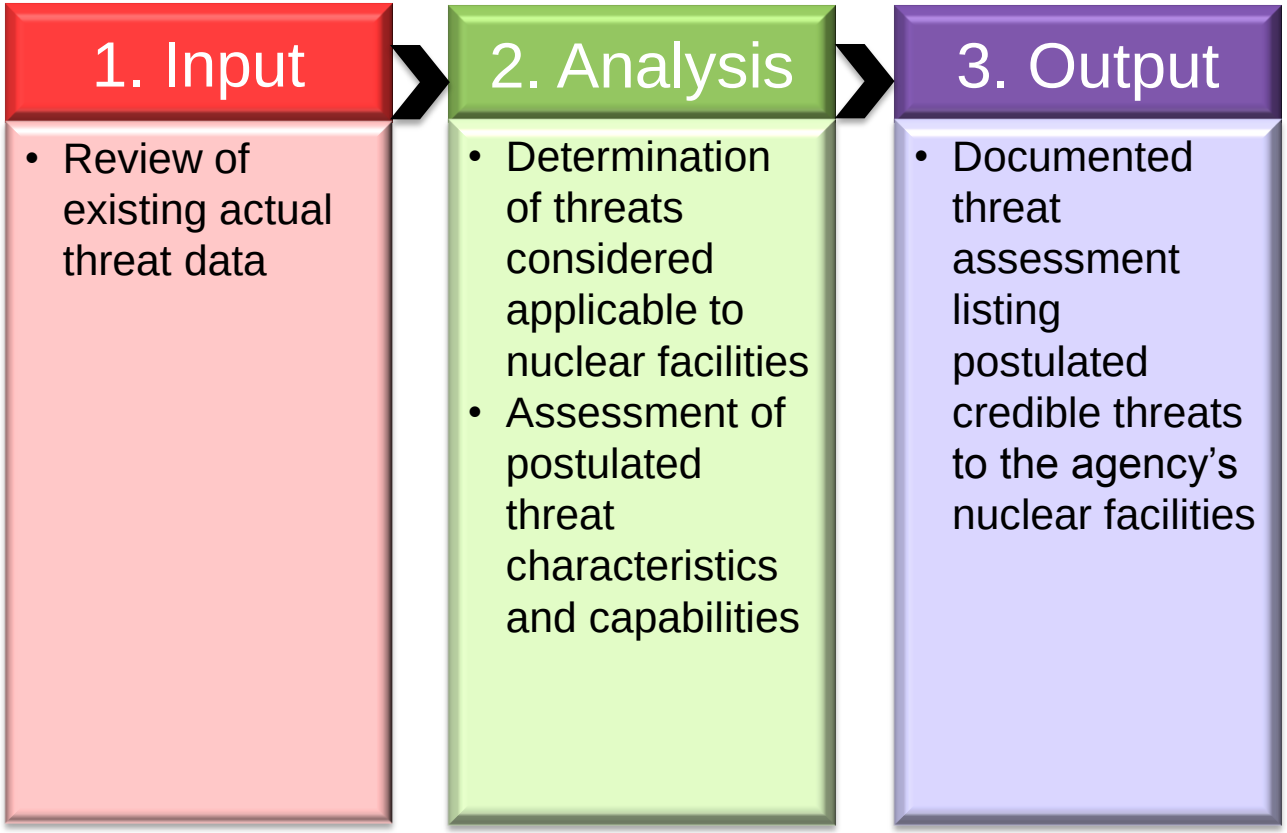
- DBT – The attributes and characteristics of potential insider and/or outsider adversaries who might attempt unauthorized removal of nuclear material or sabotage, against which a Physical Protection System (PPS) is designed and evaluated
  - Based on results of threat assessment as well as other policy considerations

Purpose of DBT

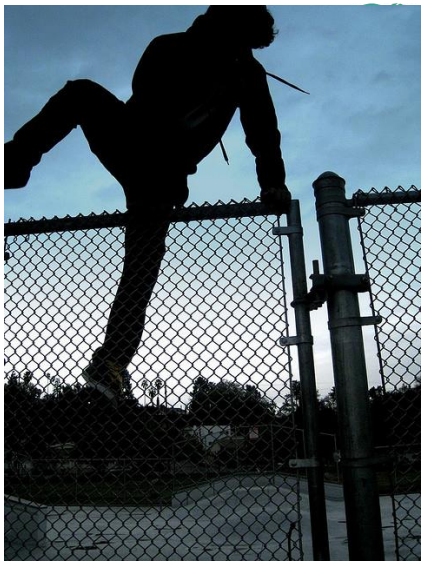
- Provides consistent policy within a country
- Provides a rational basis for
  - Evaluating the adequacy of a PPS
  - Testing and exercising
  - Supporting countermeasures modifications
  - Making and justifying decisions
- An integral input for design
- Serves as a resource management tool
  - Places reasonable bounds on effort required to protect nuclear materials
- Overall responsibility for development, implementation, and maintenance rest with a state government or agencies

Threat Assessment Process

- Threat Assessment process has three parts



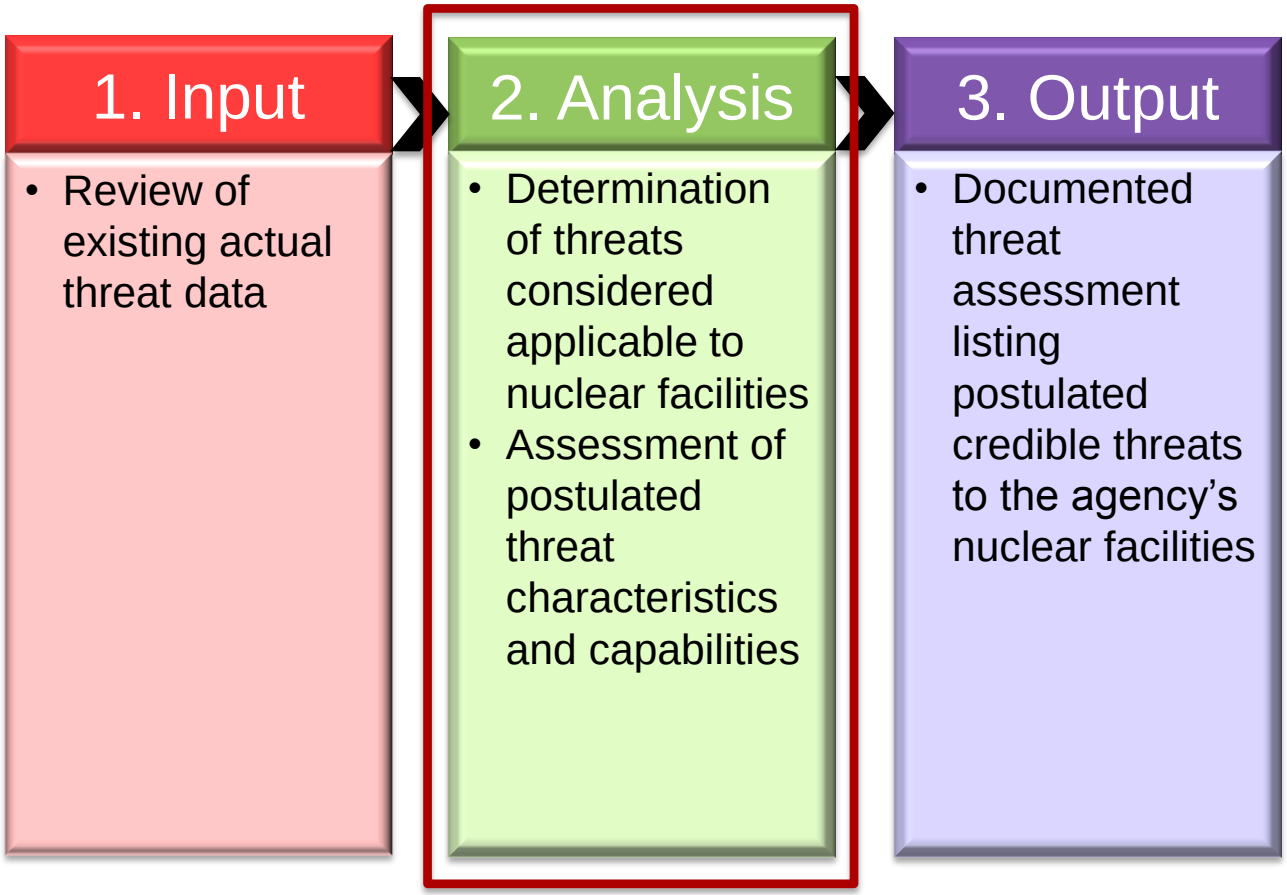
Threat Assessment Input



- Includes
  - All reliable sources of information
  - All potential adversaries
  - Local, national, regional, and international
- Considers
  - All potential adversaries' motivations, intentions, and capabilities
  - Adversaries for other high-value, high-consequences assets
  - Historical malicious acts, planned events, and training activities
  - Level of confidence for information

Threat Assessment Process

- Threat Assessment process has three parts



Threat Assessment Analysis

- Assess and document in detail each potential adversary considered applicable to the nuclear facilities

Motivation

- Political, ideological, financial, personal
- Willingness to die

Intention

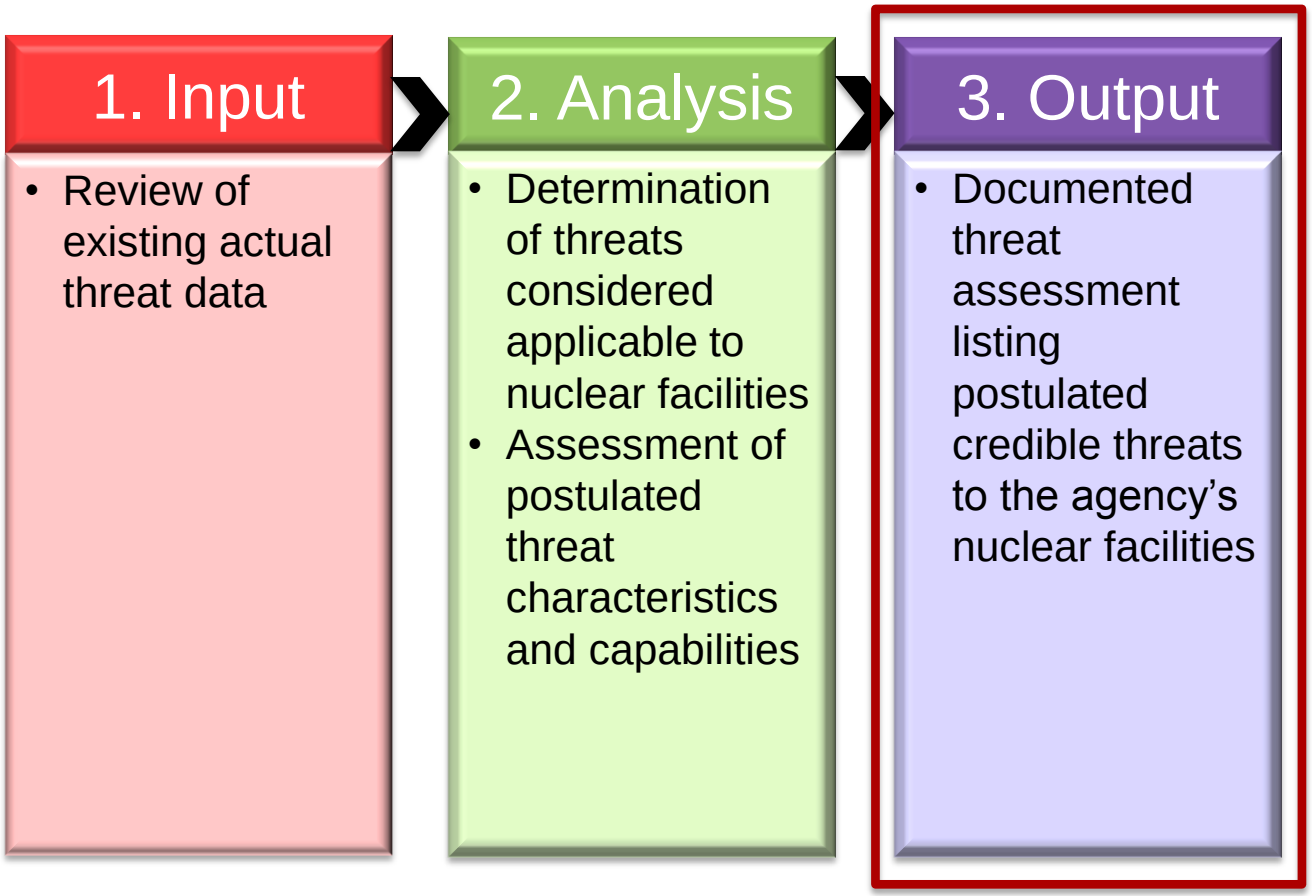
- Nuclear related
  - Theft
  - Sabotage
- Other: stop operations, social disruption, political instability, economic harm

Capabilities

- Numbers
- Weapons, equipment
- Explosives
- Knowledge, skills, and training
- Insider assistance
- Transportation methods
- Tactics

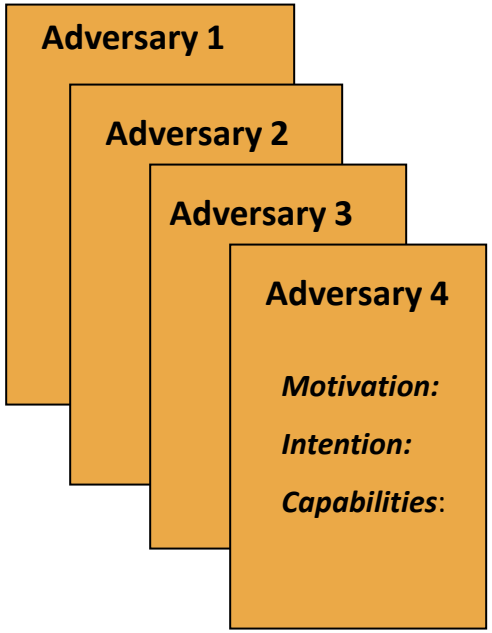
Threat Assessment Process

- Threat Assessment process has three parts



Threat Assessment Output

- Threat Assessment Output
- Contains postulated threat data to nuclear facilities under the auspices of the government agency
  - All known, credible threats applicable to nuclear facilities
  - Detailed description
  - Credibility of information
- Threat Assessment Output is an input for developing a DBT



Adversary Capabilities

- Types of adversary capabilities addressed in DBT
  - Numbers
  - Weapons
  - Equipment
  - Explosives
  - Knowledge, skills
  - Training and tactics
  - Transportation means
  - Insider assistance/collusion






Categories of Outsider Threats

- Terrorist (high-level threat)
- Criminals (moderate-level threat)
- Protestors (low- to high-level threat)
  - Demonstrators
  - Activists
  - Extremists




Terrorists

- Motivation
  - Commit violent acts to gain political objectives
- Characteristics
  - Expert use of explosives
    - Military, commercial, and homemade / improvised
  - Well funded and staffed
  - Core group may have support of a larger group
  - Military weapons
    - Fully automatic weapons, sniper, rifles, etc.
  - Wide range of transportation
  - Highly trained and motivated
  - Willing to kill and/or die

Criminals

- Motivation
  - Economic Gain
- Characteristics
  - Small group (1 to 3)
    - Organized crime may be larger group
  - Has small amounts of commercial or homemade explosives
  - Use deceit, theft, fraud, coercion, and extortion
  - Not willing to die, but may be violent to prevent capture
  - May cooperate with terrorists

Protestors

- Demonstrators
  - Motivation – Ideologically motivated
    - Looking for media attention for their cause
  - Characteristics
    - Can be small (10) or larger group (~2000)
    - Typically unarmed, nonviolent
    - Conduct acts of civil disobedience

- Activists
  - Motivation – Intent of political effect and attention of media
  - Characteristics
    - Moderate-sized group, well-educated, and trained
    - Expected to target property or police, not public
    - Cause property damage, criminal trespass

Protestors *(cont'd)*

- Extremists
  - Motivation – Intent on political effect and attention of media
  - Characteristics
    - Small group (10 to 15)
    - May have simple explosives in moderate amounts
    - May have conventional, commercially available firearms
    - Construct and use equipment in clever ways
    - Likely to be more violent than other types of protestors

Vandals

- Motivation
  - Curiosity, experimental, or desire for attention
- Characteristics
  - Small groups (1 to 3)
  - Unsophisticated and destructive in nature
  - Have no intention to injure people or cause extensive damage to targets

Psychotic

- Motivation
  - Highly motivated to achieve whatever goals are established
- Characteristics
  - Single acting
  - Suffering from mental disorder of sufficient magnitude
  - Has periodic or prolonged loss of contact with reality
  - Can be armed with a wide range of weapons
    - Handguns, rifles, shotguns, etc.
    - Conventional and / or improvised explosives

Foreign Intelligence Personnel

- Motivation – Political, loyalty to foreign country or government
- Characteristics
  - Insider Espionage
  - Have emotional ties to a foreign country or global community
  - Passive adversary
  - Function is to collect information and/or recruit insider assistance

Insider

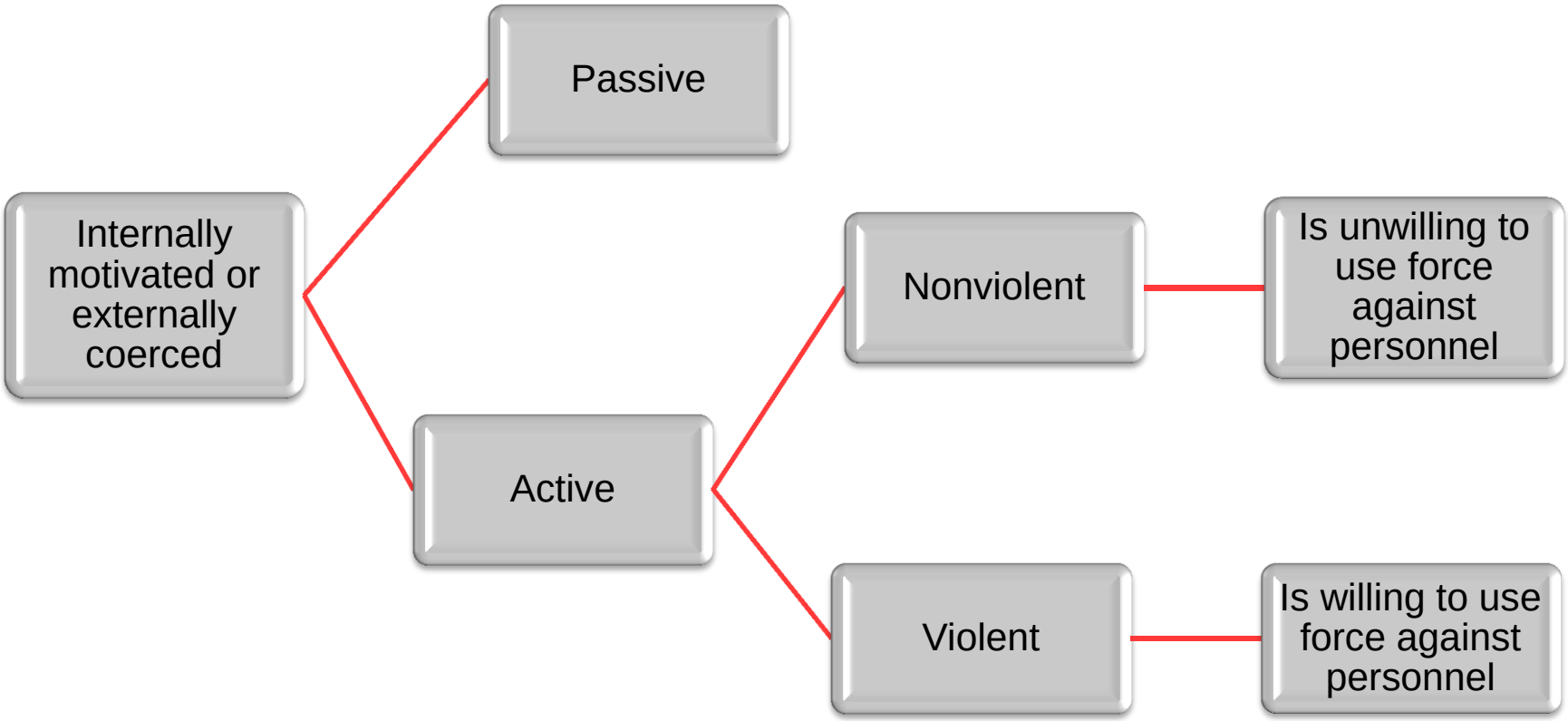
- Insider – Any individual with authorized access to nuclear facilities or transport who might attempt unauthorized removal or sabotage, or who could aid outsiders to do so
  - Looking to harm or disrupt security
- Characteristics
  - Has unescorted assess to facility and knowledge of operations
  - Most likely single acting and can collude with group of outsiders
- Insiders may include:
  - Management
  - Regular employees
  - Security personnel
  - Visitors
  - Inspectors
  - Past employees

Insider Motivations

- Ideological – fanatical conviction
- Financial – wants / needs money
- Revenge – disgruntled employee or customer
- Ego – “look what I am smart enough to do”
- Psychotic – mentally unstable but capable
- Coercion – family or self threatened
- Others?

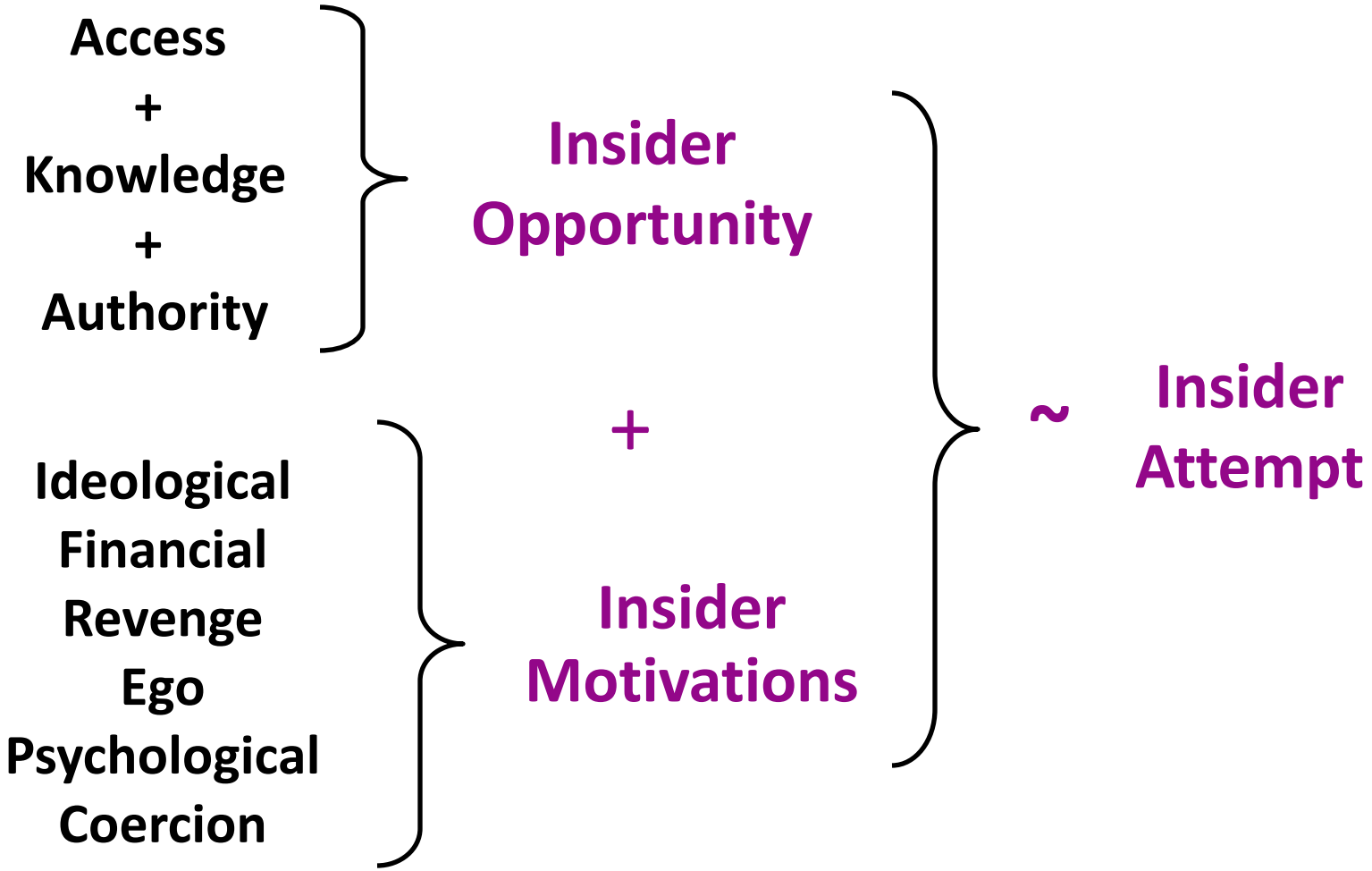
Motivation is an important indicator for both level of malevolence and likelihood of attempt

Insider Categories



All insiders can use stealth and deceit

Factors Affecting Malicious Insider Actions



Insider Access

- Authorized work areas
- Special temporary access
- Escorted or unescorted
  - Restrictions on insider during access
- Emergency access (fire, medical, police, etc.)
- Unauthorized access
  - Easy to obtain?
- Duration of target exposure
  - Conditions of target during insider access
- Protection/safety equipment and process tools
- Special site equipment
- Other?

Insider Authority

- Authority over people
  - Designated authority over others
  - Personal influence over others
- Authority over tasks and equipment
  - Assessment of alarms
  - Preparations of sensitive forms
  - Authorization of processes and procedures
- Temporary authority?
- Falsified authority?
- Exemption from procedures?
- Others?

Insider Knowledge

- Targets
  - Locations, characteristics, and details of targets
  - Details of facility layout
- Security Systems
  - Security forces capabilities and communications
  - Details of facility and security operations
  - Location and details of safety and security protection systems
- Operations and processes
  - Materials accounting
  - Operation processes
  - Tools and equipment
- Other?

Extension from Traditional Threat Assessment

- March 11, 2011 – Japan Earthquake and Tsunami
  - Caused extensive damage to Fukushima Dai-ichi nuclear reactor facility
- Natural hazards and accident are considered as part of the threat analysis evaluation

Before

After

Natural Hazards

- Generally four natural hazards used for analysis
  - Hurricane
  - Earthquake
  - Tornado
  - Flood
  - Others can be included in the analysis
- Location versus frequency of occurrence
  - Based on historic natural hazard event data
  - Estimate level of potential threat
    - Not affected = low risk

Accident Threat

- Accidents are considered to be man-induced internal or external events
  - Pipeline ruptures
  - Aircraft impact
  - Release of chemical in storage
  - Toxic release
  - Transportation accidents

- Threat environment for accidents is based on the potential for accident conditions
  - Analysis based on threat to facility or infrastructure
- Evaluate undesired events
  - Caused by severe accidents
- Unique to a specific facility or infrastructure
  - Failure of special or safety equipment

Accident Threat *(cont'd)*

- Accident condition evaluation
  - If condition is high, then risk assessment should be completed
  - If condition is low, then risk assessment not necessary

Threat Spectrum

Type of Adversary/Threat	No. of Adversaries	Equipment	Vehicles	Weapons	Motivation	Tactics	Targets of Interest
Criminal	2-3	Hand tools	Car, pickup, 4x4, truck	Handguns, automatics, knives	Financial gain. Steal property	Property theft, cyber	High-economic value assets, such as banks
Extremists	5-10	Signs, chains, locks, hand tools	Car, pickup, 4x4, truck, boat, bus	Incendiary devices, clubs	Make a political statement, protest	Protest, civil disobedience, assault, damage, destruction, cyber	Facilities with political or environmental significance
Vandals/Hackers	2-5	Spray paint, rocks, knifes	Car, pickup	Handguns, automatics	Vandalism	Damage, destruction, hacking (cyber)	Conveniently located facilities
Foreign Intel. Officer	1	Human intelligence gathering strategies	Car	Usually none	Gain access to classification/proprietary info, recruit insider	Cyber surveil., approach insider employee	Information, products, insider employee
Psychotic	1	Hand tools	Car	Up to handguns	Random	Violence, destruction	Random
Insider	1	On-site equipment	Car, pickup, 4x4, boat	Hand guns, etc.	Disgruntled	Destruction, violence, theft, cyber	Facility asset(s) and equipment, fellow employee(s)
Natural Hazards	N/A	N/A	N/A	N/A	N/A	Typhoons, Tornados, Earthquakes, Tsunamis, Wild Fires, Floods, Landslides	Critical Infrastructure, safety components
Accidents	N/A	N/A	N/A	N/A	N/A	Aircraft impacts, flooding, pipeline accidents, transportation accidents, chemical/toxic release	Critical Infrastructure, safety components

Summary

- Threat Assessment
  - Government agency-level evaluation of threats to nuclear material and facilities
  - Includes those motivation and capabilities of those threats
- Design Basis Threat (DBT)
  - The attributes and characteristics of potential insider and/or outsider adversaries against the PPS is designed and evaluated
- Types of adversary with motivation and capabilities for outsider and insider
  - Outsider
    - Numbers
    - Weapons, equipment, explosives
    - Knowledge, skills, training, tactics
    - Transportation means
    - Insider assistance

Summary *(cont'd)*

- Types of adversary with motivation and capabilities for outsider and insider *(cont'd)*
  - Insider
    - Number
    - Level of violence
- Extension from traditional threat assessment
  - Natural hazards
    - Hurricane, earthquake, tornado, flood
    - Location versus frequency of occurrence
  - Accident threat
    - Man-induced internal or external events
    - Threat to facility or infrastructure
    - Unique undesired events