



# Module 4

---

## Threat Characterization

# Threat Characterization

---

- **Design Basis Threat**
  - **Defines the threat MPC&A systems must perform against**
  - **Based on threat assessment**
  - **Periodically reviewed and revised**

# Threat Characterization

(continued)

---

- **Threat definition**
  - **Types of adversaries**
    - **Insiders**
    - **Outsiders**
    - **Insider/Outsider collusion**
  - **Range of adversary tactics**
  - **Capabilities**
  - **Motivation**

# Insiders

---

- **Definition: 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.**
- **Insiders might include:**
  - Management
  - Operations personnel
  - Security personnel
  - Service providers
  - Visitors
  - Inspectors
  - Past employees
  - Others?

# Insiders

(continued)

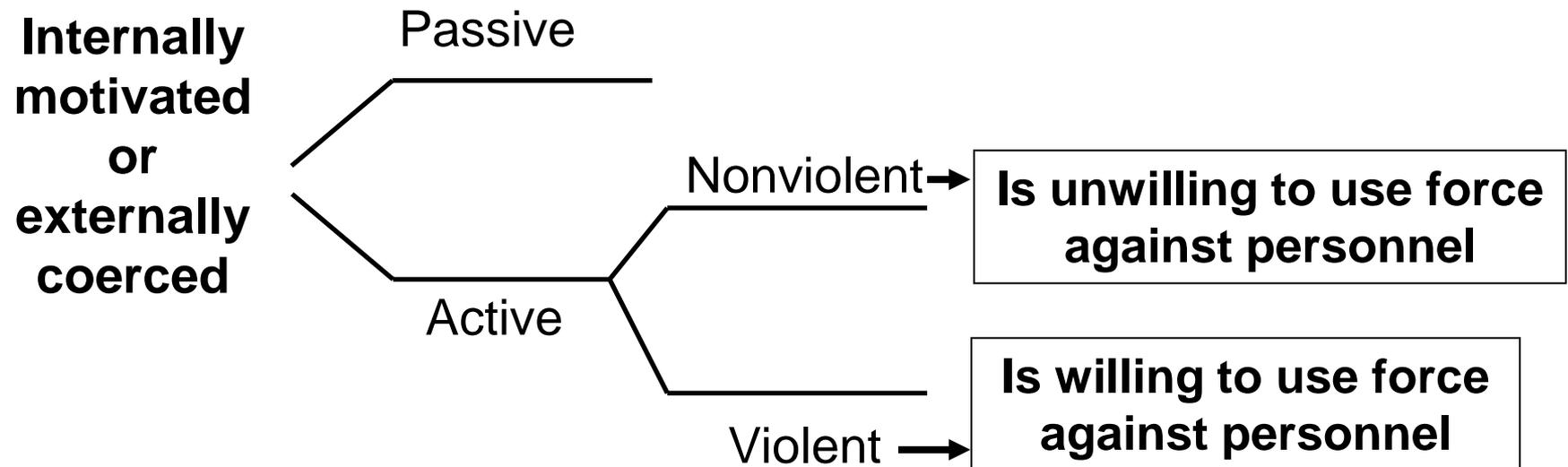
---

- **Insiders represent formidable threats:**
  - **they can often circumvent system elements**
  - **they interact directly with the target without being detected**
- **The delay and detection timelines are not as relevant because insiders can choose the most opportune times and optimum strategies**
- **Insiders can roll-up materials to acquire a goal quantity**

# Insiders

(continued)

## Categories:



- All insiders can use stealth and deceit
- Violent insiders may be rational or irrational

# Insiders

(continued)

---

## 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

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

# Insiders

(continued)

---

## Advantages:

- **Time**
  - Can select optimum time to implement plan
  - Can extend acts over long periods of time
- **Tools**
  - Has capability to use tools and equipment at work location
  - Can attempt to introduce new tools as necessary
- **Tests**
  - Can test the system with normal “mistakes”
- **Collusion**
  - May recruit / collude with others, either insiders or outsiders

# Insiders

(continued)

---

## Access:

- **Authorized work areas**
- **Special temporary access**
- **Escorted or unescorted**
  - **Restrictions on insider during access**
- **Emergency access (fire, medical, police, etc.)**
- **Unauthorized access**
- **Duration of target exposure**
  - **Conditions of target during insider access**
- **Special site equipment**
- **Accounting database**

# Insiders

(continued)

---

## 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
  - Operational processes
  - Tools and equipment

# Insiders

(continued)

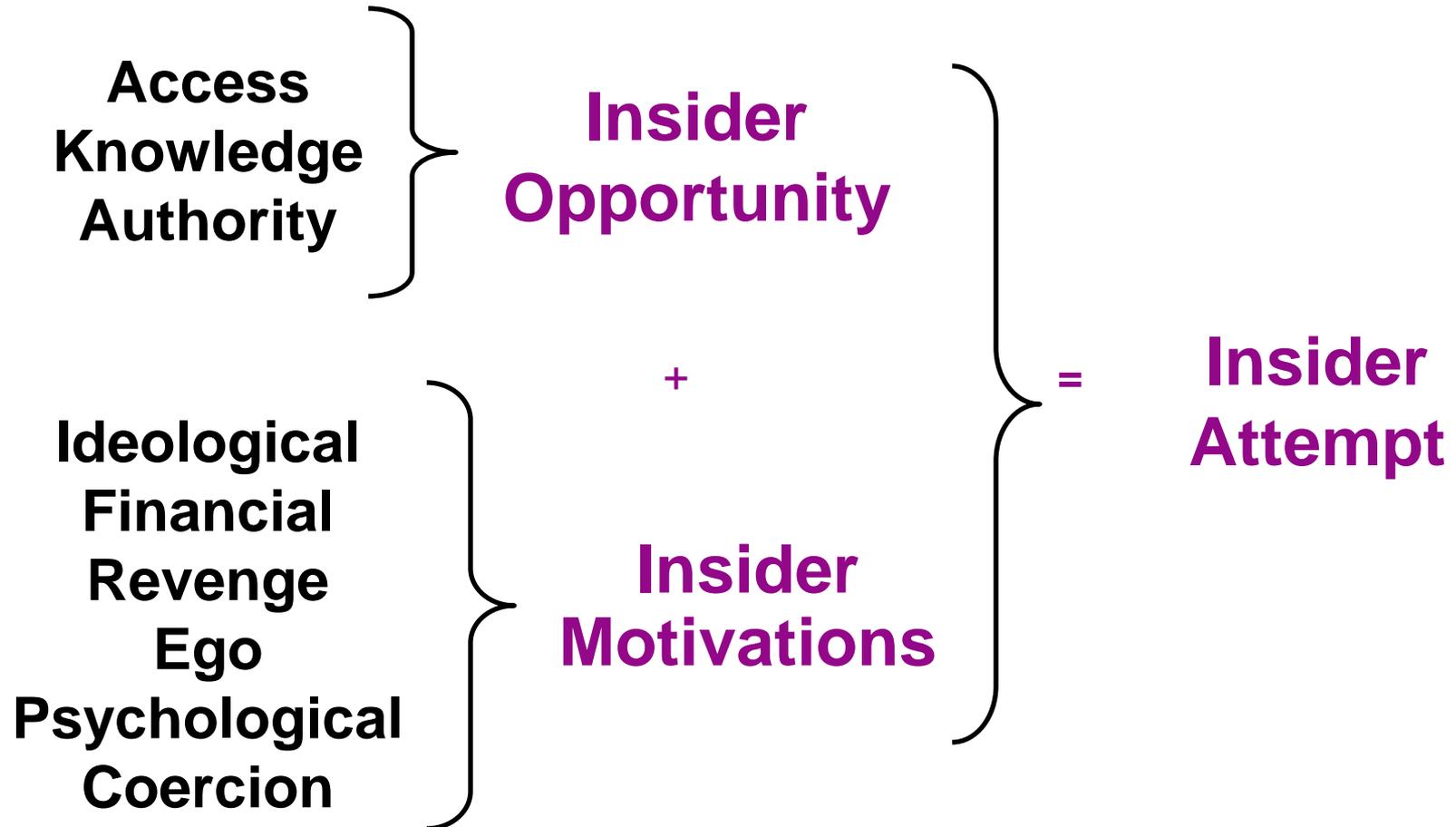
---

## Authority:

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

# Insiders

(continued)



# Outsiders

---

- **Outsider categories**
  - **Terrorists**
  - **Criminals**
  - **Anti-Nuclear Extremists**
- **Outsider motivations**
  - **Financial**
  - **Ideological**

# Outsiders

(continued)

---

- **Outsider characteristics:**
  - **Equipment**
  - **Weapons**
  - **Methods of attack**
  - **Knowledge of the facility**
  - **Insider Cooperation**
  - **Training**
  - **Funding**

# Outsiders

(continued)

---

- **Outsider Tactics**
  - **Deceit**
    - **Attempt To Defeat A Security System By Using False Authorization And Identification**
  - **Force**
    - **The Overt, Forcible Attempt To Overcome A Security System**
  - **Stealth**
    - **Attempt To Defeat The Detection System And Enter The Facility Covertly**

# Insider/Outsider Collusion

---

- **An insider's knowledge and access combined with outside resources and skills**
  - Insider can remove delay elements for outsider
  - Insider can move target partially along path, to be collected by outsider
  - Insider can defeat detection elements (CAS operator ignores alarms, maintenance technician bypasses sensors, etc.)
  - Insider can defeat access controls for outsiders (vouches for outsiders, escorts outsiders past security barriers, etc.)