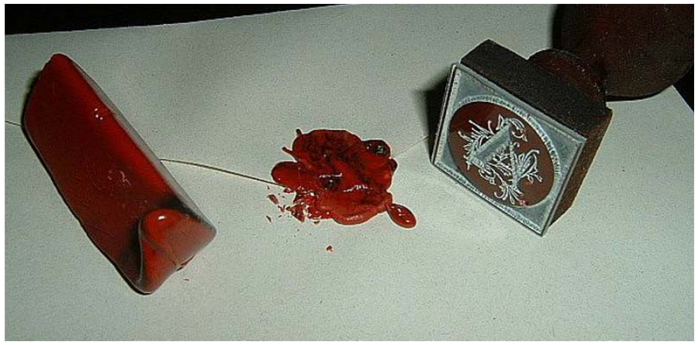
Basic Terminology – C.A. Pickett

- Tamper Indicating Device (TID)—A device designed to leave non-erasable, unambiguous evidence of access or entry.
- TID's are often referred to as **seals**, because they seal something against undetected opening.
- Unlike **locks**, TIDs are not necessarily meant to resist access, just record that it happened.



National Nuclear Security Administration

Adversary, Attack, and Insider

- The **adversary** is any person or group of people that would attempt to gain unauthorized access into a protected asset for the purpose of theft, diversion, sabotage, vandalism, or espionage.
- **Attack**—Any attempt to defeat a safeguards or security measure.
- **Insider**—A person with official access to safeguards and security information, operations, or materials.

National Nuclear Security Administration

Anomalies

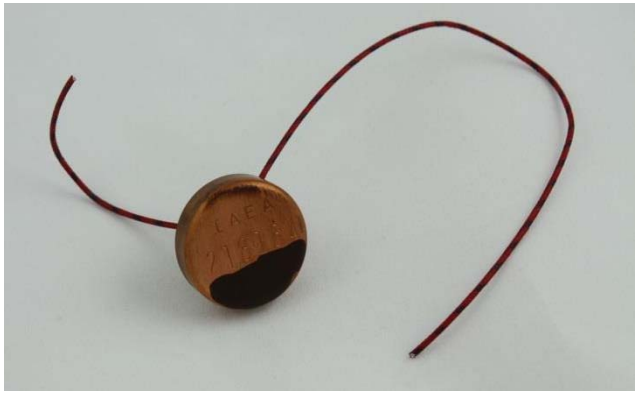
- An **anomaly** is a condition of a TID, an item, or program records requiring a response.

- Examples of anomalies include:
  - Missing, violated, or damaged TID
  - TID identifier discrepancy (TID number doesn't match records)
  - Improperly applied TID
  - Unauthorized TID
  - Uncontrolled TIDs or TID records
  - Signs of Tampering with TIDs or their markings

National Nuclear Security Administration

Integral TID Characteristics

- **Integrity** is the TID's ability to indicate that an attack has occurred.



- **Identity** is the ability of the TID to be differentiated between otherwise identically appearing TID's.

National Nuclear Security Administration

Some Basic Terminology

- Adversary - Any person or group of people that attempt to gain unauthorized access into a protected asset: for the purpose of theft, diversion, sabotage, vandalism, or espionage.
- Attack - Any attempt to defeat a safeguards/security device, layer, and/or system.
- Defeat - A successful attack of the safeguards/security device, layer, and/or system.
- Insider - A person that is officially affiliated with the organization that has access to safeguards and security information, operations, or materials and the motivation to act.
- Lock - A security device that can be opened and closed that does not provide any indication of entry. Its primary intent is to delay, complicate, and/or discourage unauthorized entry.
- Seal or TID - A device designed to leave non-erasable, unambiguous evidence of access or entry. A seal should have both **integrity and identity** as an integral part of its characteristics. **Integrity** is the seal's ability to indicate that an attack has occurred. **Identity** is the ability of the seal to be differentiated between otherwise identically appearing seals. Unlike locks, seals are not necessarily meant to resist access, just record that it happened.
- Sigillography - is the term used for the study of seals

More Terminology

- Tag – An unique assigned identifier or an intrinsic feature that is used for asset identification. Tags can be used to facilitate inventory taking, provide security, and protect against counterfeiting. Tags are typically attached to an asset and/or its containment.
- TIE - Tamper Indicating Enclosure designed to protect safeguarded items and equipment. A special kind of containment.
- Use protocol – Specifically designed procedures developed for a particular seal or safeguards/security system designed to ensure effective use of the seal.
- Authentication - is the process by which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item..
- Encryption - is the process of transforming information using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, or a key.

More Terminology

- Vulnerability Assessments (VA) – Independent assessments designed to discover weaknesses and methods for defeating particular aspects or components of a safeguards/security system.
- Red Teaming – A (VA) team dedicated to break or find weaknesses, or defeat safeguards/security system.
- Blue Teaming - A team dedicated to thwarting attackers from defeating any of the components associated with a safeguards/security system.
- Threat Assessment – A thorough analysis designed to identify and "quantify" the types of credible threats that could be deployed against a safeguards/security system. Not the same as a risk assessment!
- Passive seal – Requires physical inspection to determine breach.
- Active seal – Provides continuous monitoring of seal for breach.
- Anti-Evidence Seals – Seals that are designed to remove or erase specific information or features upon opening.

Material Control typically refers to: Containment & Surveillance

- *Containment:* Control, hold, surround, and limit

  "Protect"

- *Surveillance*: Observation, close watch, or examination with scrutiny

  "Chain of Custody"

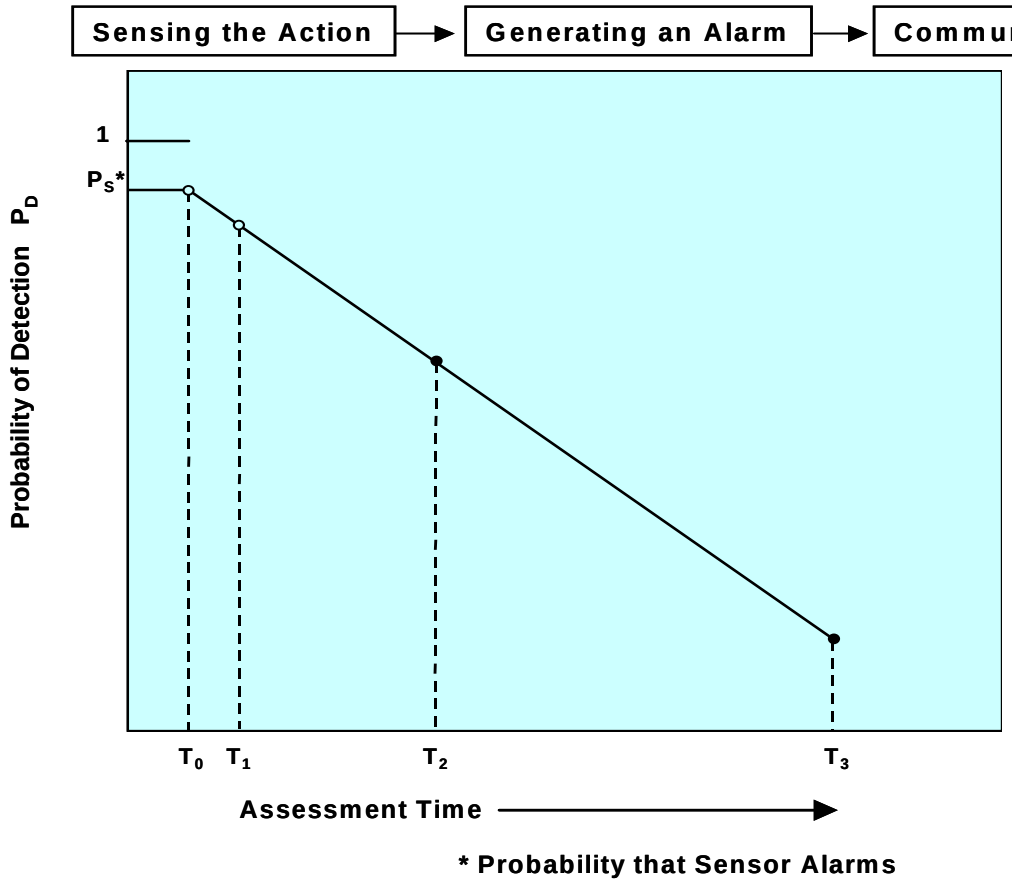
  "Continuity of Knowledge"

Provide assurance that the recorded measurements are still valid!

Together work to Detect Theft or Diversion

Detection

- **Detection** is the discovery of an adversary action. It includes sensing of covert or overt actions. To discover an adversary action, the following events must occur:



• Detection will decrease as assessment time increases because the more time required to make an accurate assessment, the less likely the alarm will be properly assessed

Definitions

- Access Control – The process of permitting access or denying access to information, facilities, special nuclear materials, resources, or designated security areas
- Anomaly – Anything observed in the operation or documentation of safeguards and security systems that deviates from expectations based on previously verified conditions or documentation
- Daily Activity Check (DAC) – A daily review to provide timely identification of obvious abnormalities or missing items, or to ascertain that there is no indication of tampering (i.e., Active TID systems, unattended systems, etc…).

National Nuclear Security Administration

Some Tools for Detecting Insider Activity

- Human Reliability Program (HRP) – A security and safety reliability program that ensures individuals who occupy positions affording access to certain materials, nuclear explosive devices, facilities, and programs, meet the highest standards of reliability and physical and mental stability
- In Process Inventory – The amount of special nuclear material in a process area at any specified time
- Process Monitoring – A system of monitoring production data (e.g., flow rates, yields, densities, etc.) and of production control or quality control measurements that can help detect and resolve an anomaly that may be an attempt to divert or take material.

National Nuclear Security Administration

Definitions

- Two-Person Rule –A teamwork principle based on the requirement that at least two duly authorized people must be present simultaneously in one work location in order to decrease the probability of unauthorized actions
- Waste – The nuclear material residues that have been determined to be uneconomical to recover (but must be under MC&A material control program)

National Nuclear Security Administration

Material Control Goals

- **Nuclear Materials Control** – The part of the domestic safeguards program that provides the protocols (checks and balances) for all nuclear material activities:
  - Provide “chain of custody” monitoring (who, what ,where, & when)
  - Govern movement, location, and use of the materials
  - Monitor inventory and process status
  - Provide indicators and potential detection of unauthorized activities
  - Provide methods to analyze and resolve inventory difference and anomalous events.

National Nuclear Security Administration

Moving toward a goal of Continuity-of-Knowledge (CoK)

CoK for Safeguards Purposes:

- is the outcome of a system of data or information regarding an item or activity that is uninterrupted and authentic that provides adequate insight to draw definitive conclusions that nuclear material is not being diverted from peaceful purposes.

It is important to note that:

"CoK is an outcome, not a process"

National Nuclear Security Administration

Containment & Surveillance

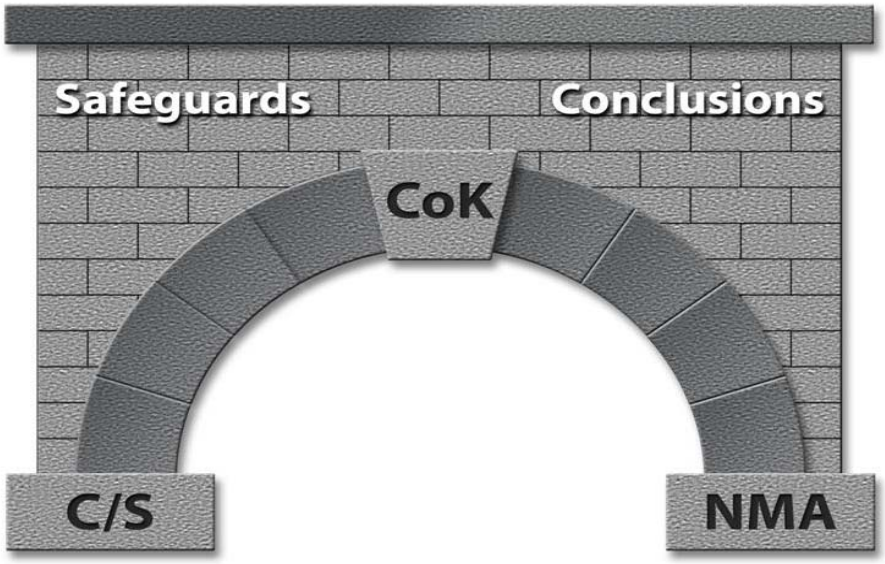
- Containment and Surveillance (C/S) technologies are part of integrated system approaches designed to provide "continuity of knowledge" of declared nuclear assets and activities.
- C/S technologies have increased importance for arms control efforts since many measurement-based techniques may be considered too intrusive.

The function of any safeguards Containment and Surveillance (C/S) system is to collect information that can be used to verify activities at a nuclear facility.

- Containment systems represent systems and technologies that are designed to provide secure methods that control, surround, protect, and some cases delay access to nuclear assets. The primary purpose of containment is to facilitate the accountancy and security of nuclear assets.

CoK is the Keystone for Drawing Safeguards Conclusions

Built on a foundation of nuclear material accountancy (NMA) and containment and surveillance measures (C/S), Continuity of Knowledge (CoK) provides the confidence to support a safeguards conclusion.



As reliance shifts to CoK information takes on equal or even primary role to NMA in drawing safeguards conclusions

National Nuclear Security Administration

Surveillance and Unattended Monitoring

- **Surveillance systems** are basically technologies and methodologies designed to watch and record as many activities and attributes as possible associated with nuclear materials and processes. The goal for these systems is essentially to be the **"inspector's eyes in the field"** or to provide verification that activities are occurring as declared.
- It is desired that C/S systems be designed to support **remote unattended monitoring**. This can reduce the need for accessing areas where operational activity is limited.
- Future facilities and processes should consider unattended systems that can provide real-time monitoring of processes, stored assets, and transfers.
  - Safeguards by Design