Overview of Information Barrier Concepts

Presentation to the
International Partnership for Nuclear Disarmament Verification, Working Group 3

Michele R. Smith
United States Department of Energy
NNSA Office of Nuclear Verification

Geneva, Switzerland
September 2016

Background Information

The Challenge:

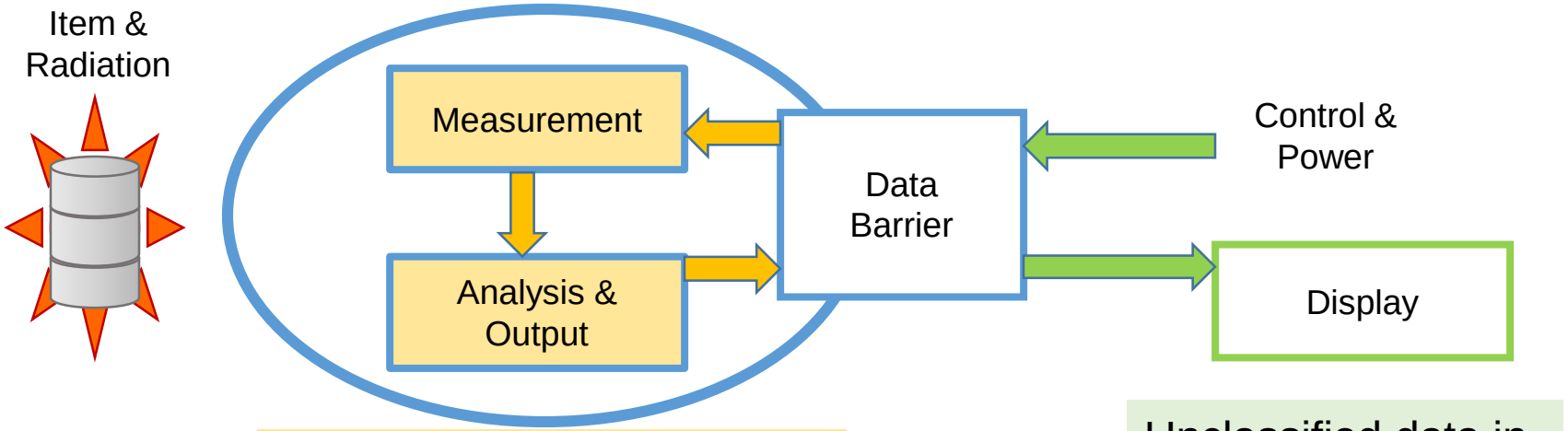
- Implement high-quality measurements to provide confidence/assurance in monitoring of classified/sensitive items to build international confidence
- Protect highly sensitive design information to address nuclear nonproliferation and security concerns

The U.S. began studying the ideas behind information barriers (IB) in the context of international treaties and agreements in the mid-1990s

There has been considerable development of IB concepts and approaches in international contexts both in exercises and agreements

Information Barriers

- Provide accurate and reproducible information on nuclear weapons and sensitive items
  - Monitoring party requirement for inspection system or inspection processes
- Assure protection of classified nuclear weapons design information or other sensitive information
  - Host requirement to prevent disclosure to monitoring party



Barrier Elements protect potentially classified data

Unclassified data in open areas

What is an "Information Barrier"

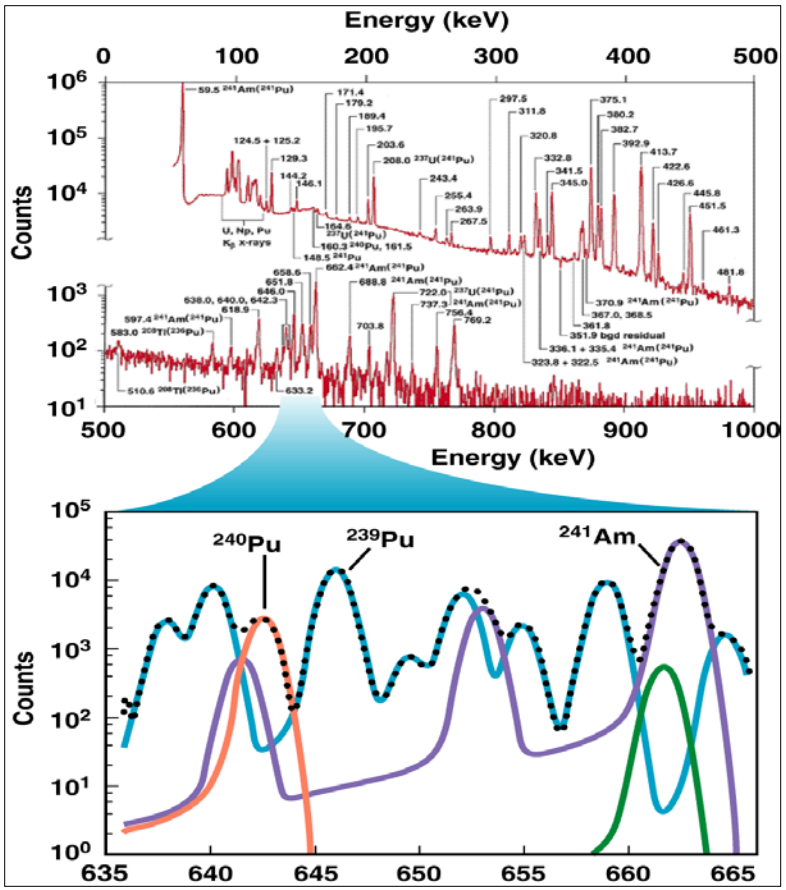
An information barrier is:

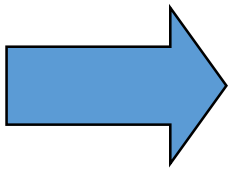
- a combination of *technology* (hardware and software) and *procedures* (administrative controls) to prevent the release of classified information while allowing meaningful measurements and independent conclusions [Close, 2001]
- a combination of physical and/or encryption mechanisms that preclude acquisition of sensitive, quantitative information [Bachner, 2013]

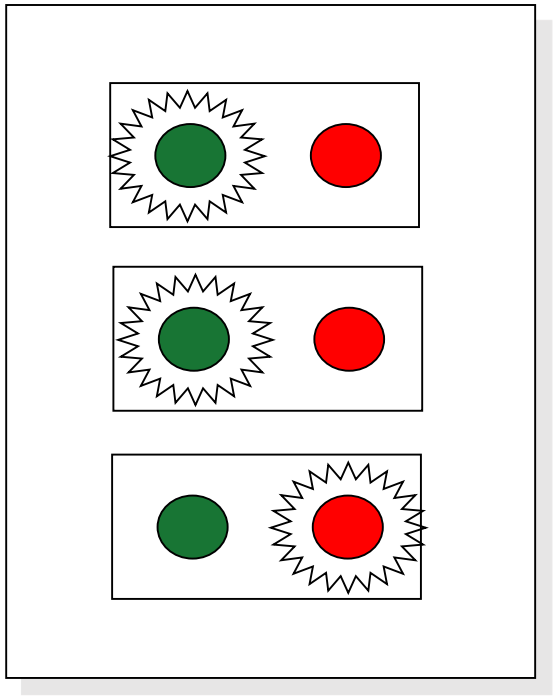
*An information barrier is designed to **provide confidence** that the measurement system **functions as designed** and as implemented to **provide accurate and reproducible information** on nuclear weapons or sensitive items.*

Information Barriers

Classified measurement results are compared to unclassified threshold values to obtain an unclassified pass or fail result







Implications of the Definition of Information Barrier

- Information Barriers are not a single monolithic technology that protects sensitive information
- The idea of the Information Barrier indicates the tension that occurs in a monitoring regime
  - The needs of the monitoring party versus the needs of the monitored party

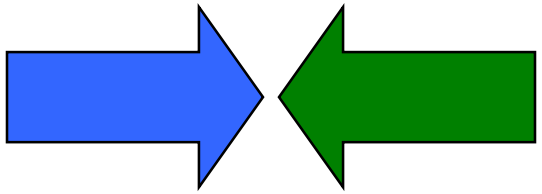
Divergent goals in monitoring regimes

Monitored Party

Competing Goals

Monitoring Party

Protection of classified information



Confidence in measurement

The monitored party must be assured that its classified information is protected from disclosure to the monitoring party.

The monitoring party must be confident that the integrated system measures, processes and presents the conclusion in an accurate and reproducible manner.

The requirement to protect the classified information of the monitored party is paramount to any regime.

Conflicting goals in a monitoring regime

- Clearly competing goals in a monitoring regime cannot be fully reconciled
- Confidence can be increased for both parties by implementing technical and procedural measures
- The monitored party's concerns may be addressed by certification and implementation of information barriers
- The monitoring party's concerns may be addressed by implementing authentication procedures throughout the technology development and implementation
- Both party's issues may be addressed by joint development and joint demonstrations

Approach to developing a robust IB

- **Measurement/regime requirements**
  - Establish measurements to be taken & scenarios for taking them
- **Information protection requirements**
  - Identify sensitive information that is vulnerable in the process
- **Protection features available**
  - Consider the combination of software, hardware & procedures
- **Information barrier design as a system**
  - Explain how features protect each item of sensitive information
- **Independent vulnerability assessment**
  - Critical review of effectiveness of barrier in protecting information

IB Design Considerations

- Joint development between the monitored and monitoring parties ensures full understanding of the features included
- Simple is better
  - Fully transparent
  - Ease of inspection
  - Modular design
    - Single function modules
  - Open source software
    - i.e. Procedural languages rather than object oriented
  - Commercial equipment may include unwanted functionality
- Implementing International Standards for hardware and software

IB Procedural Considerations

- Configuration control process
- Full documentation
- Strict protocol for dealing with party that has last access to technology
- Acceptance testing with *certified* standards to exercise the monitoring technology

IB Design Considerations

Design Element	Issue	Design Solution
Equipment Certification	Host's security concerns and operational safety issues with equipment	Enable host certification of equipment (with supplier and design considerations)
Central Processing Unit (CPU)	Implementation of unknown, complex, multi-functional processor in equipment	Minimize extraneous functionality and maximize inspectability in hardware and software architecture of CPU
Non-CPU Equipment	Implementation of unknown, complex, multi-functional non-CPU elements	Minimize extraneous functionality and maximize inspectability of non-CPU elements
Procedural Issues	Monitor's deduction of classified information from experimental setup and conduct of operations	Automate instrument measurements and reduce operational input of equipment
Electronic Emanations	Manipulation or recording of electronic emanations from measurement system	Understand and control measurement system emanations and interferences

IB Design Considerations

Design Element	Issue	Design Solution
Intermediate Barriers	Host's security concerns with protection of classified information	Optimize security of system through placement of multiple barriers while maintaining system functionality
Software, Firmware, Operating Systems	Risk of compromising or manipulating classified information through computer codes	Minimize extraneous and complex code to maximize inspectability and protection of classified data
Inputs and Outputs (I/O)	Risk of compromising or manipulating classified information through I/O peripherals	Implement simple, dedicated and functionally-defined I/O peripherals. Eliminate undefined, extraneous I/O peripherals.
Measurement System Authentication/ Repair	Monitor's assurance in functionality and integrity of system to present accurate and reproducible conclusion on classified item	Implement inspection/ authentication protocols for software and hardware that provide optimal review of system and subsystems

Example: Importance of simplicity

Consider the complexity of common software and hardware

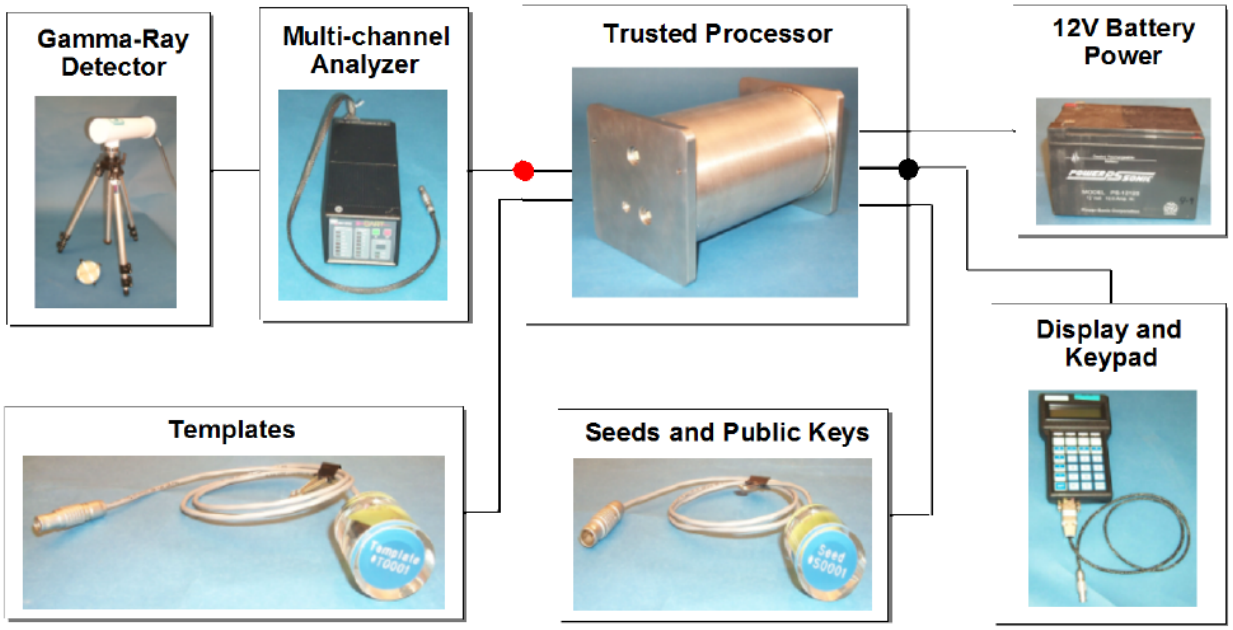
- Software (minimum executable size)
  - Windows Vista — 20 billion bytes
  - Windows NT Embedded — 8 million bytes
  - MS/DOS — 200 thousand bytes
  - eCos — 4 thousand bytes
- Hardware (number of transistors)
  - Core i7 — 781 million transistors
  - Pentium IV — 42 million transistors
  - 80486dx — 1.2 million transistors
  - LEON Processor — 140 thousand transistors

Propagation of complexity is not simply additive – it propagates like the sum of squares

Simpler systems are cheaper and faster to authenticate

Example: Trusted Radiation Identification System (TRIS)

- **Hardware** components >>
- **Software** Algorithms:
  - authenticate software
  - generate encrypted keys
  - generate digital signatures
  - verify template signature data



TRIS generates and confirms radiation templates for classified items

TRIS incorporates design options to protect classified information and cryptographic functions for authentication of software and radiation signature templates

Summary

- Information barriers provide a means to provide confidence in monitoring of classified/sensitive items through high-quality measurements and protection of sensitive design information
- An information barrier addresses the challenge of divergent goals for monitored and monitoring parties in any monitoring regime
- Special considerations for information barriers:
  - Never reveal classified information
  - Inspection technology should be autonomous and independent of item configuration
- The successful implementation of technology can bridge the opposing goals of the parties in a monitoring regime
  - Joint development and demonstration may ease both party's misgivings about the monitoring technology
- Information barriers can protect classified/sensitive information but require continual development that considers technology advancements