LA-UR-17-21911
Approved for public release; distribution is unlimited.

Title: Two-Black Box Concept for Warhead Verification

Author(s): Bates, Cameron Russell
Frame, Katherine Chiyoko
Mckigney, Edward Allen
Smith, Morag Kristin

Intended for: Program Review

Issued: 2017-03-06

Los Alamos
NATIONAL LABORATORY
EST.1943

Delivering science and technology
to protect our nation
and promote world stability

NNSA
National Nuclear Security Administration

Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA

Two-Black Box Concept for Warhead Verification

State Department Verification Fund Review

Cameron Bates, Katherine Frame, Edward Mckigney, Morag Smith

3/9/2017

Los Alamos NATIONAL LABORATORY EST.1943

NNSA National Nuclear Security Administration

Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA

Outline

- **We have created a possible solution to meeting the requirements of certification/authentication while still employing complicated criteria**
  - We have specifically addressed the question of nuclear warhead verificiation
- **The team at LANL included members from NEN-2 and XCP-3 who have been involved in various aspects of arms control research including the WMC, NA-243 projects, and E2E**
- **Technical solutions to protecting information from the host in an inspection environment needs to be assessed by those with specific expertise but, LANL can still study the verification problem**
- **This concept intentionally keeps analysis hidden from host**
  - Provides ambiguity
  - Allows for complex analysis
  - Requires analysis be jointly destroyed after measurements
- **Follow on**
  - Work with NA-243 to further develop details
- **The two-black box framework developed provides another potential solution to the confidence vs. certification paradox**

The confidence certification paradox in warhead verification

- **The host wants to be able to certify that the measurement is not revealing classified information**
- **The monitor wants to be able to have confidence that the item is a warhead**
- **If the host knows the monitor's methods they can design spoof items**
- **Once the monitor loses physical control of the instrumentation, verifying that the instrumentation has not been tampered with is difficult**
  - Simple discrete analog components
  - Tags and seals
- **Traditional solutions have focused on relying on simple attributes but this limits the confidence when the host knows what is being evaluated**

The team involved in the two-black box project

- **Katherine Frame (PI):Developed the plan for this project, provided technical expertise in aspects of certification in real nuclear facilities**
- **Edward McKigney: Provided technical expertise related to analysis techniques of data measured in arms control scenarios**
- **Morag Smith: Provided technical expertise on concepts of operations in warhead verification scenarios**
- **Cameron Bates: Lead technical work on project. Provided technical expertise in data acquisition and analysis**

Project Execution

- **Funded for FY16 originally**
- **NA-243 and WMC work delayed progress**
  - Practical aspects are tied tightly to real implementation issues
- **Previous NA-243 study was finished in FY2016**
- **This work fit appropriately been previous study and next study**
  - De-conflicting funding and limiting cross-iteration
- **We will produce document on study results before the end of FY17**

What is new about the two-black box concept

- **Split the measurement system into three components**
  - Measurement hardware – jointly designed built by monitor installed at host facility permanently (Radiation detectors, X-ray machine)
  - Open measurement acquisition and analysis – jointly designed and permanently installed (Power supplies control software, data acquisition, agreed upon analysis)
  - Closed analysis – Monitor brings to inspection, connects to open measurement and analysis. Both parties verify expected behavior. Perform verification.
  - Destroy hardware to satisfaction of both parties
- **This technique enables more complex analysis**
  - Only computational limitation is what can be put in the box
- **This adds ambiguity to what is being assessed**
  - Much more difficult to have confidence in a spoof
- **Any classified information derived from analysis is destroyed along with the box**
- **Monitor has confidence in box because they maintain control over it until it is destroyed**

Non-destructive assay equipment

- **Neutron detectors**
  - Presence of neutron sources (include U, Pu) and limited information about their configuration
- **Gamma-ray detectors**
  - Detect unique emissions from radioactive isotopes
  - Determine ratios of different radioactive isotopes
  - Detect presence of hydrogenous material via capture gamma-rays
- **X-ray imaging**
  - Tells difference between high-Z and low-Z materials

- **Jointly designed by monitor and host**
- **Built by monitor**
- **Brought to facility and certified by host**
- **Tags and seals installed by monitor**

These instruments are illustrative not a requirement

Open Analysis

- **Neutron detectors**
  - Calculate moments of the neutron multiplicity
- **Gamma-ray detectors**
  - Calculate isotopic ratios given known detector efficiency curve
  - Calculate absolute emission rate for each gamma-ray energy
- **Radiography**
  - Acquire data and process image to pass to closed analysis
- **Data quality/instrument performance checks**
- **COTS hardware**
- **Jointly designed by monitor and host**
- **Built by monitor**
- **Brought to facility and certified by host**
- **Tags and seals installed by monitor**

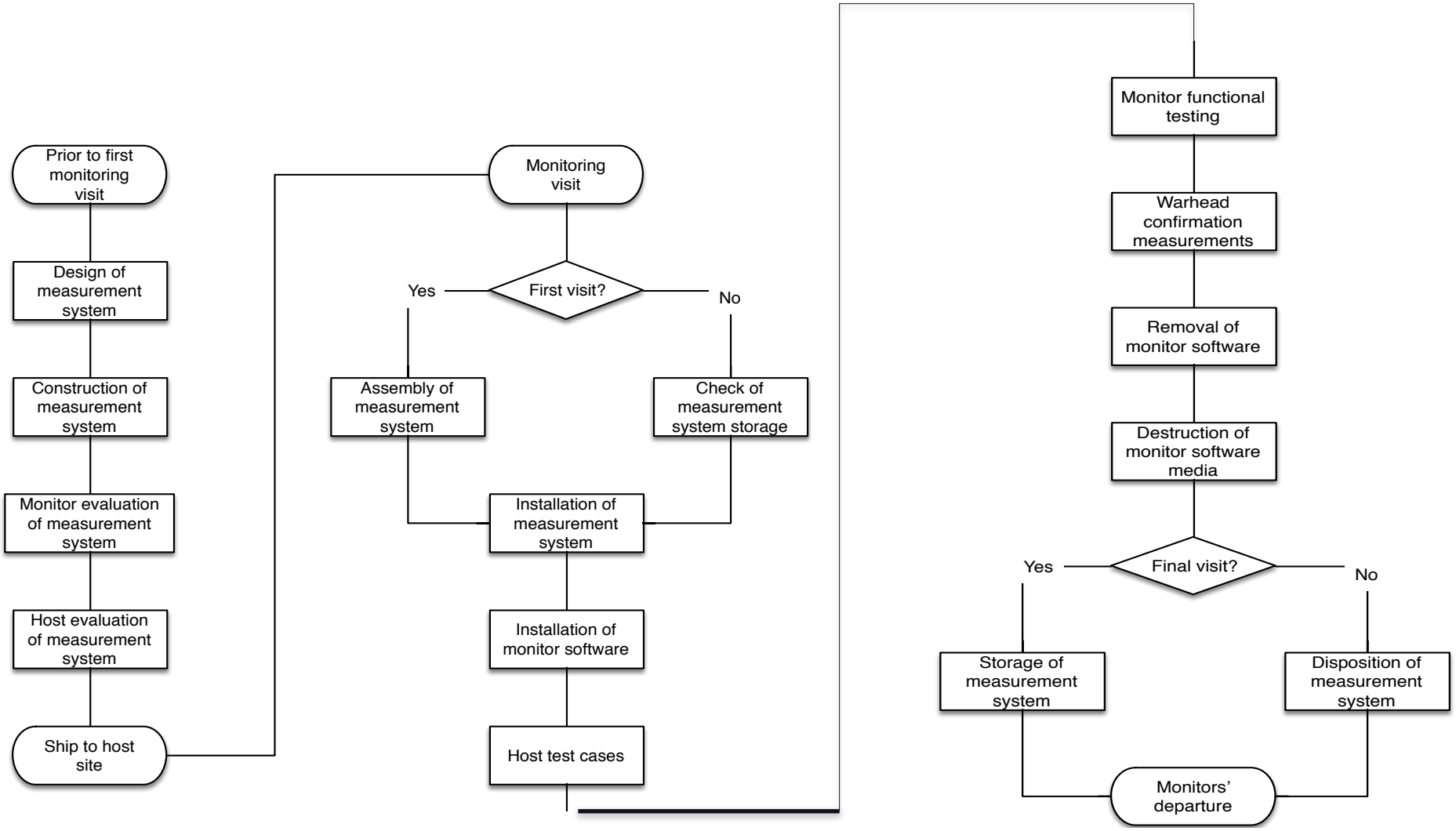
Closed Analysis (the “black-box”)

- **Combine data from all open analysis in closed analysis box**
- **Example:**
  - Calculate $^{239}Pu/^{240}Pu$ ratio from gamma-ray spectrum
  - Calculate fissile mass from neutron multiplicity analysis
  - Use multiplicity/neutron rate along with capture gamma-rays to calculate hydrogenous moderator thickness
- **Portable hardware**
  - Harden against electronic attack
- **Encrypted software**
  - Protection from host
- **Verifiable destruction:**
  - Ball mill (turn hardware to dust)

Protecting information on the black box

- **After scoping the problem and consulting subject matter experts at LANL we realized that anything more than notional concepts are better left to appropriate agencies**
- **How hard this is depends on how analysis is treated**
  - Is it state proprietary information
    - No consequence beyond the treaty itself if host accesses information
  - Is it classified
    - At what level
- **Our basic concept**
  - Data exists on encrypted internal flash drive that requires some multi-factor authentication from monitor to be decrypted
  - Data resides in memory unencrypted during the analysis process
  - Box is a faraday cage with hardened power supply input
  - Data from open analysis is transmitted via fiber
- **Is this enough?**

Concept of operations



Conclusions and Future work

- **The two black-box concept is one possible solution to aspects of the certification/authentication problem**
- **No fundamental limitations to bringing a "black-box" into a US facility**
  - Likely additional precautions would be necessary
- **Protection of information stored on a disk that has to be accessed during the monitoring process is non-trivial**
  - LANL overestimated our ability to address these issues ourselves (underspent)
- **The concepts developed here will be further elaborated on in a follow-up study looking at a more specific implementation with NA-243**