LA-UR- 10-03607

Approved for public release;
distribution is unlimited.

Title:	Random Selection as a Confidence Building Tool
Author(s):	Duncan MacArthur Danielle Hauck Diana Langner Morag Smith Jonathan Thron Richard Williams
Intended for:	The 51st Annual INMM Annual Meeting

Los Alamos
NATIONAL LABORATORY
EST. 1943

Form 836 (7/06)

RANDOM SELECTION AS A CONFIDENCE-BUILDING TOOL

Duncan MacArthur, Danielle Hauck, Diana Langner, Morag Smith, Jonathan Thron, and Richard Williams

Los Alamos National Laboratory
PO Box 1663, MS E540, Los Alamos, NM 87545, USA

ABSTRACT

Any verification measurement performed on potentially classified nuclear material must satisfy two seemingly contradictory constraints. First and foremost, no classified information can be released. At the same time, the monitoring party must have confidence in the veracity of the measurement. The first concern can be addressed by performing the measurements within the host facility using instruments under the host's control. Because the data output in this measurement scenario is also under host control, it is difficult for the monitoring party to have confidence in that data. One technique for addressing this difficulty is random selection.

The concept of random selection can be thought of as four steps: (1) The host presents several "identical" copies of a component or system to the monitor. (2) One (or more) of these copies is randomly chosen by the monitors for use in the measurement system. (3) Similarly, one or more is randomly chosen to be validated further at a later date in a monitor-controlled facility. (4) Because the two components or systems are identical, validation of the "validation copy" is equivalent to validation of the measurement system. This procedure sounds straightforward, but effective application may be quite difficult. Although random selection is often viewed as a panacea for confidence building, the amount of confidence generated depends on the monitor's continuity of knowledge for both validation and measurement systems.

In this presentation, we will discuss the random selection technique, as well as where and how this technique might be applied to generate maximum confidence. In addition, we will discuss the role of modular measurement-system design in facilitating random selection and describe a simple modular measurement system incorporating six small ^{3}He neutron detectors and a single high-purity germanium gamma detector.

THE CHALLENGE

Most treaty monitoring scenarios can be reduced to two requirements:

- The owner of nuclear material or a device (the host party) makes a declaration concerning that item to another entity (the monitoring party).
- The monitoring party must verify this declaration without observing any classified information.

The crux of the treaty-monitoring problem lies with the final phrase "without observing any classified information." Traditional nondestructive assay (NDA) techniques (based on gamma detection,

neutron detection, or calorimetry) are widely and successfully used in numerous scenarios (e.g., waste assay and spent fuel monitoring) that do not involve classified information.

In these situations with no classified material or information, the type of system shown schematically in Fig. 1 meets the declaration/verification requirements. The declaring party and the verifying party can use NDA instrumentation, either jointly or separately, to observe all of the relevant information concerning the nuclear material (or waste) in a sealed container.

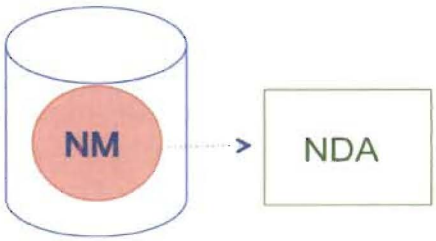

Fig.1. Traditional NDA techniques used in an open environment where there are no classification concerns.

The simple process shown in Fig. 1 breaks down if a classified nuclear item is present in the sealed container or system. In this case, even though the NDA instrumentation may be similar or identical, the output cannot be shared directly with the monitoring party. One way of protecting the classified information is to introduce an information barrier (IB) that surrounds the classified material and any measuring electronics that might contain classified information. This IB is shown conceptually in Fig. 2.

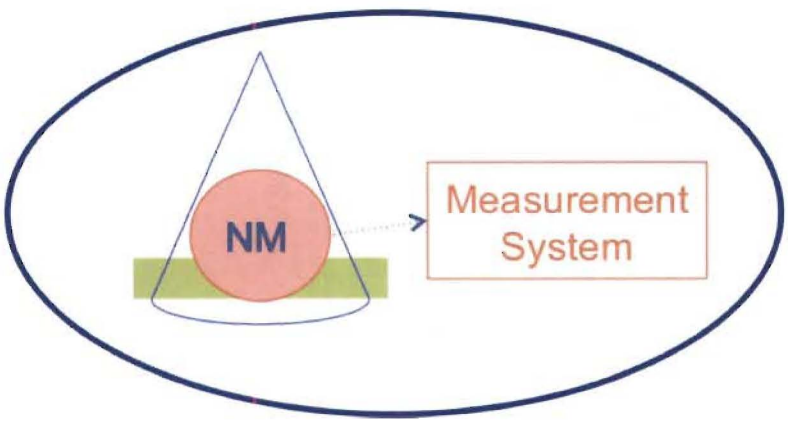

Fig. 2. Conceptual IB. All classified information is kept inside the barrier, and the monitoring party is kept outside.

In practice, an IB is not the single shell shown in Fig. 2. The practical IB includes layers of hardware, software, and procedural protection to provide a barrier system that, as a whole, is fault resistant and

the components of which are fault tolerant. This approach results in a classified information system that is not prone to single-point failures.

THE ATTRIBUTE MEASUREMENT SYSTEM

Unfortunately, the same IB system that excels at protecting the host party's classified information also excels at "protecting" the monitoring party from any information that could be used to confirm the host party's declaration. One way to allow a carefully controlled information release from inside the IB is to use the attribute measurement system (AMS) shown in Fig. 3.

Attributes, as measured in an AMS, are unclassified indicators of potentially classified measurement results. Potentially classified information can be made into an attribute by comparing the information with a threshold, i.e., the attribute is "quantity above threshold." Some potential attributes are the

- presence of nuclear material,
- nuclear material mass above a threshold,
- plutonium isotopic ratio below a threshold, or
- uranium enrichment above a threshold.

In any fielded implementation of an AMS, the host and monitoring parties would agree on the attributes to be measured (as well as the details of the AMS itself).

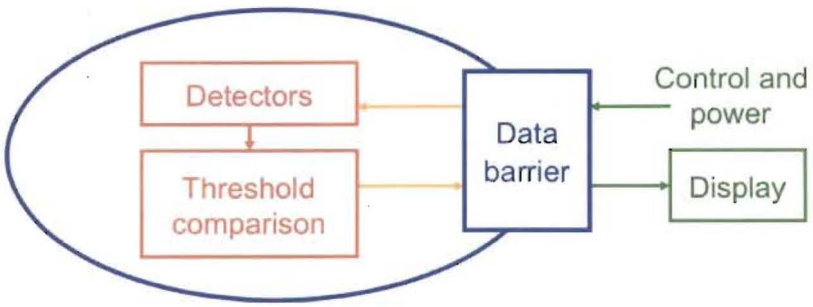

Fig. 3. An example of a generic AMS. In this case, potentially classified information is compared with a previously agreed-on threshold to generate an unclassified attribute. Only these unclassified attributes can pass through the data barrier to be displayed as red/green lights.

COMPETING CONCERNS

The host and monitoring parties often will have different concerns when addressing the declaration/verification challenge. The host party must be assured that classified information cannot be released. This concern typically is addressed through the process of system certification. At the same time, the monitoring party needs to be able to draw independent conclusions concerning the veracity of the material declaration. The monitoring party achieves the required confidence through the process of authentication. Although the red-light/green-light display shown in Fig. 4 may satisfy

the host party's certification requirements, such displays may not generate sufficient monitor confidence in the measurement system.

Fig. 4. Typical attribute display panel. Even displaying multiple attributes may not generate the same level of confidence as traditional data displays (e.g., neutron count rate or gamma spectra).

RANDOM SELECTION

Scenario—Random selection, as applied to confidence building, can be quite straightforward in concept. In implementing this technique, separate randomly selected copies of a system or component are used both for measurement and for validation. One useful scenario for random selection might work in this manner:

- Several identical copies of a component or system are presented.
- One (or more) is randomly chosen for use in the measurement system.
- One (or more) is randomly chosen for validation.
- If the two remain identical, validation of the "validation copy" is equivalent to validation of the measurement system.

This process allows for effective validation of the measurement system without requiring monitor access to the measurement system after classified measurements have been made. Because neither party knows beforehand which items will be chosen for validation or measurement, it is more difficult to modify the measurement system without simultaneously modifying the validation system.

Although the selection process by itself is not an authentication technique, effectively implemented random selection can be used to change the constraints placed on the authentication procedure by time and access limitations. Applications of random selection to increasing confidence depend on the ability, or perceived ability, of the monitoring party to completely validate a component or system (the validation copy) given enough time and access. In particular, random selection of components or systems can move the time and place of the authentication from the host facility during a monitoring visit to a monitor facility at a different time.

Thus, by effectively applying this process, validation could be accomplished at a monitor-owned facility rather than in a host-owned facility. However, any authentication advantage gained depends

on the ability to know that nothing has changed (maintain continuity of knowledge) with either the measurement or the validation systems following the selection process. Even if the two pieces of equipment were identical at the time of selection, effective application as an authentication tool requires that the two remain the same. This equality can be particularly difficult to maintain if the measurement system is a large piece of equipment located in a host-controlled facility many miles from the border of the host country.

The random selection process is often viewed as a panacea. As described above, random selection does not "solve" the authentication problem; instead, random selection changes the problem, making some parts (e.g., time and access constraints) easier and some (e.g., continuity of knowledge) more challenging. Thus, random selection should be viewed as one very useful authentication tool as opposed to a complete solution. Available authentication tools include

- random selection,
- cooperative design,
- design transparency,
- validation techniques,
- continuity of knowledge, and
- functional testing.

The combination chosen will depend on the requirements placed on the particular monitoring regime and on negotiated positions.

Validation—As mentioned above, the selection process by itself is not an authentication or validation technique. Random selection can be used to change the constraints of the validation process (i.e., the timing, location, and security constraints of the validation). However, the random selection has not eliminated the need for validation. The original hardware and software validation issues still exist, although they are transferred in time and space.

Having said this, transferring the validation procedure to a monitor-owned facility is potentially very important. Complete hardware and software "reverse engineering" is possible given sufficient time and access. Both could be available in a monitor-owned facility.

Measurement System Design—If used correctly, random selection is a powerful authentication tool. To most effectively apply random selection, features should be incorporated into the measurement system design to facilitate both the selection process and the maintenance of the required continuity of knowledge.

Assembling an AMS out of multiple smaller modules, rather than creating it as a single monolithic design, has several advantages for the random selection process:

- Transporting smaller modules back to the monitor's facility is an easier logistics problem.
- It is possible to select pieces of the system for validation rather than the entire measurement system.
- Producing multiple copies of the modules for random selection would be less expensive than producing multiple copies of the entire system.

Although size was not explicitly considered in earlier designs, system size and, in particular, smallest module size are important when designing for ease of random selection. Although a lack of complexity is still a useful feature, it has been overtaken by size as an authentication concern. If a small item can be validated in a monitor-owned facility, the complexity of that item is less important. Larger systems, in particular neutron counters, can be broken into several individual modules that would then be assembled into a complete measurement system in situ. Validation of one module, or several modules, would increase confidence in the measurement system without requiring random selection of, and maintaining continuity of knowledge on, an entire measurement system. However, the modules cannot be too small. During the random selection process, small items could be harder to keep track of—potentially losing the continuity of knowledge.

An example of a modular neutron detector is shown in Fig. 5. If such a detector were used, the modules, rather than the (large and expensive) detector, would be the unit for selection.

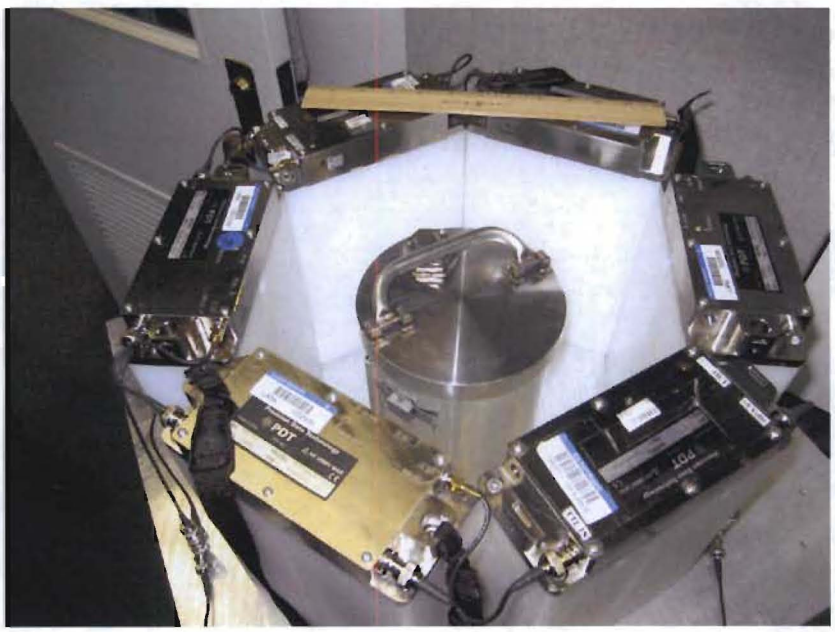

Fig. 5. Example of a small modular neutron detector. This system is made up of six individual polyethylene "slabs." The high-purity germanium detector is located under this neutron detector.

ACKNOWLEDGMENT

This work is supported by the United States National Nuclear Security Administration's Office of Dismantlement and Transparency.