LA-UR-99-5634 (Rev.)
February 2000

Fissile Material Transparency Technology Demonstration Attribute Measurement System with Information Barrier: Functional Requirements

Rena Whiteson and Duncan W. MacArthur
Los Alamos National Laboratory
October, 1999

I. INTRODUCTION

For the purpose of this paper, we have used the term "functional requirement" to indicate a required function rather than the recommended method for performing that function. The information barrier (IB) is part of an entire Attribute Measurement System (AMS). The creation of effective AMS/IB technology will proceed through the following steps:

1. AMS/IB Functional Requirements,
2. AMS/IB hardware and software specification,
3. AMS/IB hardware and software construction, and
4. AMS/IB implementation.

II. GOAL OF THE ATTRIBUTE MEASUREMENT SYSTEM WITH INFORMATION BARRIER

The goal of the AMS/IB is twofold:

1. to guarantee that only agreed-upon unclassified data are displayed and that no classified data can be assessed or revealed, and
2. to provide assurance that the unclassified data output accurately reflects the classified data input.

III. ASSUMPTIONS

1. Measurements
    a. Some unclassified identifiers (such as container ID) will be measured.
    b. Some classified identifiers (such as radiation signatures) will be measured.
    c. No classified information will be revealed to inspecting parties.
    d. Verification system operation may be checked (e.g., by inserting blind standards into the measurement area) by either party at any time.
2. Data
    a. Classified data will not be transmitted out of the AMS/IB.
    b. No Classified data will be archived.
    c. Unclassified output may be archived together with container identification.
    d. Archived unclassified data must be in a form that is unalterable by either party but readable by both parties.
3. Equipment
    a. All inspection equipment will be under dual control; maintenance can be performed only when the inspected and inspecting parties are represented.
    b. The system can be sanitized.
    c. Commercial hardware is employed to the maximum extent practical.

IV. FUNCTIONAL REQUIREMENTS

We have divided the functional requirements for the information barrier into the following areas:

1. Physical Protection,
2. Hardware Emissions Control,
3. Assurance of Capabilities and Limitations,
4. Administrative Controls,
5. Validation and Verification of the Systems and Data,
6. Error Detection & Resolution,
7. Equipment Sourcing and Maintenance, and
8. Data Paths (intended and unintended).

Additional discussion of the reasons for and rationale behind this AMS/IB concept is included in the Appendix.

1. Physical Protection

- Access control through technology and procedures of both hardware and software must prevent unauthorized access and tampering.
- Any unclassified data archives will be handled appropriately and will be protected against surreptitious modification.

2. Hardware Emissions Control

- A barrier between the detectors and the display should minimize both transmission from the detectors to the outside and from the outside to the detectors.
- Consider transmission through the air (e.g., rf radiation).
- Consider transmission through conductors (e.g., power-supply wiring).

3. Assurance of Capabilities and Limitations

- The level of understanding required of any given element depends on the location of that element; if an element is located so that it cannot release classified information, then the handling of classified information by that element is less critical.
- The barrier described in section 2 should eliminate the possibility of transmission of classified information.
- The capabilities and vulnerabilities of commercial software and hardware that could be used by the system must be understood.
- The capabilities and vulnerabilities of custom task-specific software and hardware must be understood.
- The capabilities and vulnerabilities of the entire analysis system must be understood.

4. Administrative Controls

- Procedural rules must be in place for participant activities.
- Procedural rules must be in place for maintenance procedures.
- Continuity of knowledge (of system operation) must be achieved (and recorded).
- All participants will agree on levels of participation in all activities.
- Operational security must be maintained.

5. Validation and Verification of the Systems and Data

- Hardware and software inspection and verification are essential.
- Functional testing of the analysis system is essential.
- It must be possible for all parties to authenticate any archived data.

6. Error Detection & Resolution

- A procedure for handling system errors must exist. This procedure should address
  - misidentification of an object under test,
  - detection of an error condition, and
  - rectification of errors without revealing classified information.
- A procedure for handling measurement errors must also exist. This procedure should address
  - identification of an error type or condition and
  - a remeasurement protocol.
- Understand the effects of each type of error. In particular, consider both
  - false negatives and
  - false positives.

7. Equipment Sourcing and Maintenance

- Use commercial hardware, if practical.
- Allow for manufacturer maintenance of commercial hardware, if possible.
- Use commercial software, if possible.
- Keep commercial software as simple as possible.
- Minimize the use of custom hardware and software.
- Keep specialized hardware and software as simple as possible.
- Allow for sanitation of all of the system.

8. Data Paths

- The IB is a combination of hardware and software barriers.
- The unclassified display cannot control the operation of the classified detector systems.
- The amount of classified data at each stage of the system will be reduced to the minimum required to allow correct functioning of the system.
- Use the principle of defense-in-depth to reduce both the probability and consequences of any inadvertent information release.
- Protect hidden data paths.

- Maintenance operations must be accommodated.
- Even if individual elements are secure, interaction between elements may create pathways for the loss or diversion of classified information.
- Minimize barrier crossings. Each crossing is a potential route for information loss or covers manipulation.

APPENDIX

Introduction

The primary goal of the AMS/IB that is described in this document is to eliminate **any** possibility of the release of classified information from the measurement system to any outside party while allowing the collection of useful data.

While preventing the release of classified information, the AMS/IB must also enable the inspectors to be confident that the unclassified output correlates with the classified input. These two goals are generally competing and mutually exclusive.

Finally, the need for verification of nuclear materials will extend for many years. Thus, any AMS/IB will need to be useful for a long time. The requirements that must be addressed include: (1) the continued availability of essential parts used in construction of the system, (2) the ability to easily upgrade the system as new techniques and abilities become available, and (3) the maintenance that is required for long-term operation of electronics and nuclear detectors.

Attribute Measurement Systems with Information Barriers

As illustrated in Fig. 1, an AMS/IB can be thought of as a box (the IB) with the measuring and computational systems on the protected side (inside) and the display on the open side (outside). All classified data generated by the measurement system will remain inside the box. There are three types of routes for unintentional classified information release across the IB.

1. Some data must be passed through the IB in order for the inspector to receive useful information about the inspected object. Although these data themselves are unclassified, care must be taken to ensure that classified information does not “leak” through this connection.

2. All other connections (e.g., power supply) or operations (e.g., maintenance) that pass through the IB are also potential conduits for classified information transfer or manipulation. The connections can be addressed by hardware controls and the operations by access controls. However, the most straightforward way of minimizing the potential for classified data leakage or modification is to minimize the number of barrier crossings.

3. Energy (e.g., acoustic, optical, radio-frequency) radiated from the inside to the outside of the box could also carry classified information. Since there is no intentional transmission across the barrier, the simplest solution is elimination of all transmission. This can involve a combination of hardware and access controls.

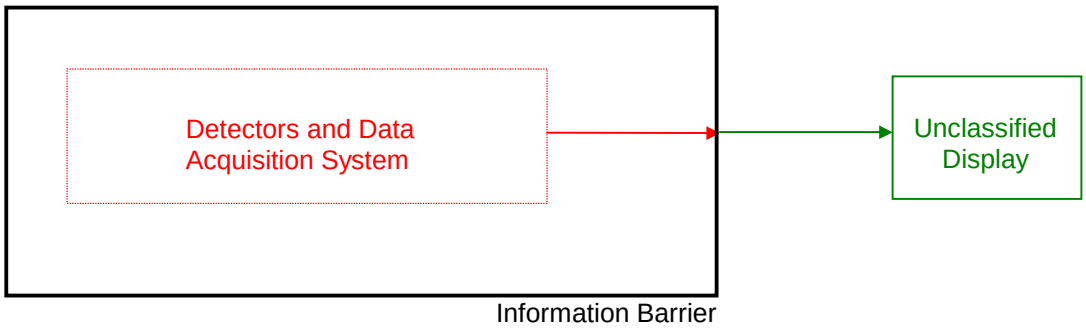

Fig. 1. Conceptual AMS/IB system for protection of classified information. Everything inside the IB "box" is protected as classified; everything outside is treated as unclassified. Any connection between the inside and the outside, either physical or administrative, offers the potential for classified information transmission or manipulation.

An effective AMS/IB will incorporate a suite of controls, both (1) administrative and access, and (2) hardware and software. As with many operations, the types of controls can be ordered (from most preferred to least preferred):

1. elimination of the problem or transfer mode,
2. substitution of another method to achieve the desired result,
3. hardware or software elimination of the problem, and finally
4. administrative or access control to eliminate the problem.

Thus, although administrative and access-control solutions to a problem are often the easiest, these types of solutions are the least reliable type and should be considered only if no better method is available. They are perhaps most useful in combination with hardware and software solutions. People are fallible, especially in long-term operations; thus, any solution relying solely on people presents an opportunity for failure.

Although the IB "box" of Fig. 1 is a useful tool for locating and minimizing vulnerabilities, this concept is overly simplistic and prone to single-point failure. A complete AMS/IB can incorporate a series of data-filtering stages followed by a final barrier to prevent the release of any classified information. The data filtering reduces the amount of classified information available throughout the detector system(s) through proper choice of detection methods, hardware discriminator settings, data processing methods, etc. Thus, the IB consists of several layers of protection rather than a single layer. The sum of all the layers ensures that no classified information is released. The multi-layer approach can provide the same amount of protection as a single layer, but without the single point failure mode inherent in a single-layer design. The end result is that no classified information is displayed in the open area.

Inspector access to facilities where verification is carried out is expected to involve restrictions on the materials that the inspectors may bring into and remove from the facilities. The controls will also govern the activities permitted. Examples of such restrictions include requirements for declaration of all items being brought in or requested for removal from the facility, examinations of all items declared, and physical access

restraints including clothes changes and searches for undeclared items. In controlled-access locations within facilities, inspectors will be under continuous supervision of facility security staff.

The host nation may determine that inspector access controls and/or additional physical protection must be provided for any or all components of the AMS/IB. This may include items such as NDA instruments, computers, and connectors. Vaults, security guards, surveillance systems, locks, tamper-indicating seals, or similar devices can be used to guarantee that hardware and software have not been modified or tampered with in any way since last verified by all parties.

Additional protections can be provided administratively when verification implementation arrangements are developed for each specific facility. This may be accomplished with a detailed procedures rulebook specifying allowed behavior of inspectors and facility operators during inspections, during routine maintenance, and at other times considered necessary. An activity log may be maintained to provide continuity of knowledge.

Administrative controls will also be required in order to maintain operational security. Inspectors will not be allowed to bring uncontrolled radiation detectors into the inspection area. Uncontrolled detectors could include active devices (such as portable detectors brought in to check the response of the main system) as well as passive systems (such as film badges or other instruments that record personal dose or dose rate).

Attribute Measurement

An attributes measurement system incorporates direct measurement of several radiometric properties (or attributes) of an object with comparison of these quantities with agreed-upon unclassified thresholds. The results of these comparisons are the unclassified “attributes” of the object.

The six attributes that have been chosen for plutonium measurement for The Fissile Material Transparency Technology Demonstration are:

1) presence of plutonium,
2) plutonium isotopic ratio,
3) plutonium mass,
4) plutonium age,
5) presence of oxide, and
6) symmetry of plutonium.

One possible implementation of the AMS/IB concept is illustrated in Fig. 2. In this figure, the data-barrier element in the data-output connection is explicitly called out. The data barrier is a simple (and hence easily validated) element residing on the IB whose only function is to ensure that no classified data are passed into the open area. An AMS/IB based on this concept can explicitly contain examples of many of the types of

controls mentioned above. Many of the information filters, particularly those relating to detector choice, eliminate the possibility of transfer of excess classified data by eliminating any method of collecting those data. Data filters that limit the collection or transmission of classified data in hardware (e.g., discriminator settings) are examples of hardware controls; data processing that generates quantities such as isotopic ratios is an example of a software control. The administrative and access control elements of the IB also serve to prevent the release of classified information. Figure 2. Shows an extension of the simple AMS/IB concept. Although only one layer of protection is shown, this represents multiple layers that must be implemented in the AMS/IB.

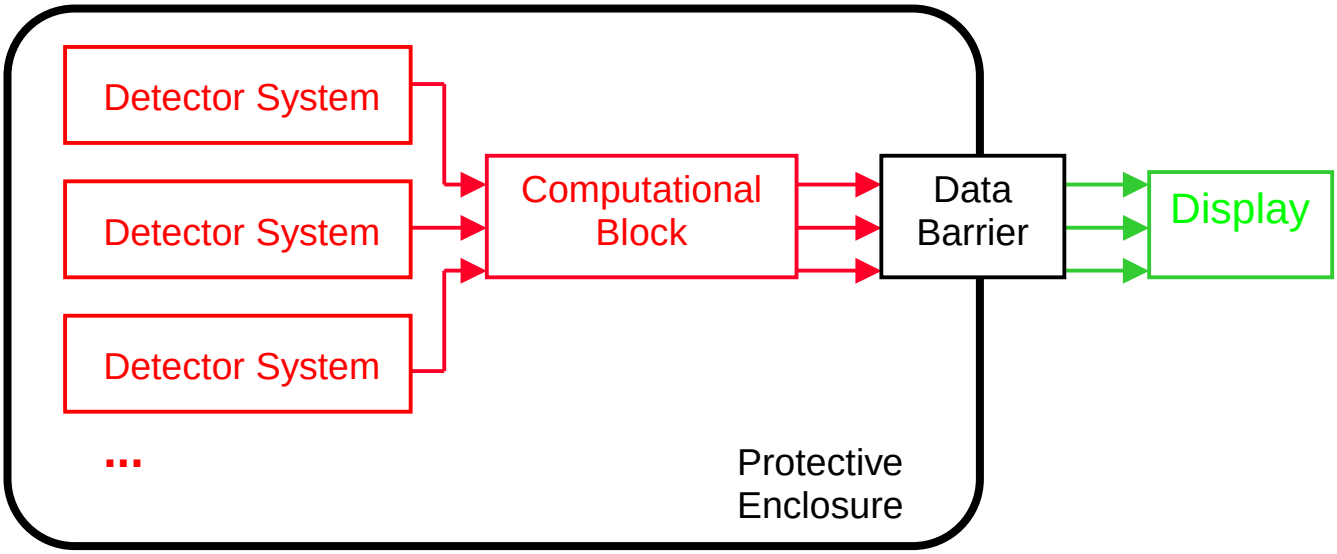

Fig. 2. Extension of the simple AMS/IB concept illustrated in Fig. 1 illustrating additional detail. The attribute measurement detectors, the attribute comparison block, and the data barrier are shown explicitly.

Authentication of the AMS/IB is important for acceptance of the system. Authentication is the process of demonstrating that the outputs from the system do, in fact, accurately reflect the contents of the objects presented to the system. Two methods of authentication (which might be used in concert) are (1) blind testing and (2) detector system authentication. Although neither of these methods is ideal, a combination may produce acceptable results.

1. A truly blind test would involve inspector presentation of an object, the contents of which were unknown to the inspected State. The correct identification of the contents would add confidence that the system was operating correctly. However, in reality, the State controls and must track the plutonium that would be used in this test object. Thus, a truly blind test may involve complex procedures or may not even be possible, depending on the material accounting and physical protection rules of the State.

3. When no classified material or classified data are present, the inspector could verify the operation of each stage of the detector system(s) using unclassified sources. In this case, complete output (spectra, multiplicities, shape, etc.) should be be available to allow inspector comparison with the attributes of the known reference object

A combination of these techniques would involve on-site authentication of the unclassified reference materials using inspector supplied equipment. Even though the host supplies the reference material, the inspecting party can draw totally independent conclusions as to what is in the reference material and how the AMS/IB should react..