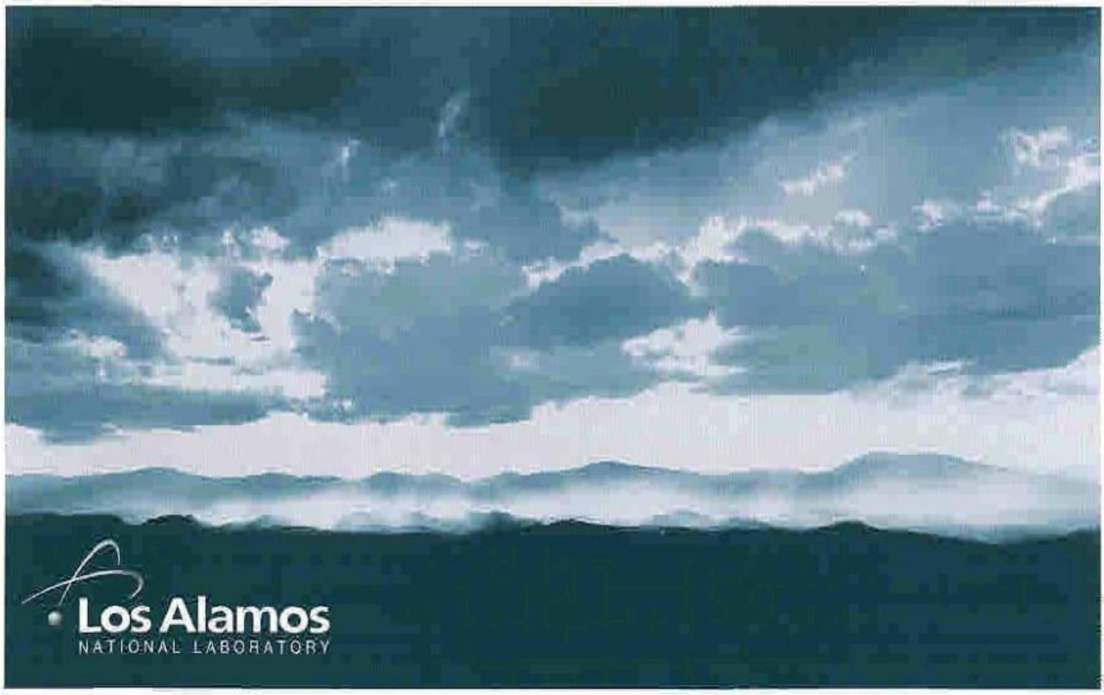
LA-UR-05-4149

ADVANCES IN INFORMATION BARRIER DESIGN

Richard B. Williams, Kate C. Frame, Robert P. Landry,
Duncan W. MacArthur, and Morag K. Smith
Safeguards Science and Technology Group (N-1)
Nuclear Nonproliferation Division
Los Alamos National Laboratory
Los Alamos, NM 87545

Presented at the
Institute of Nuclear Material Management
46th Annual Meeting
Phoenix, Arizona
July 10-14, 2005



Chris J. Lindberg

LA-UR-05-4149

ADVANCES IN INFORMATION BARRIER DESIGN

Richard Williams, Kate Frame, Robert Landry, Duncan MacArthur, and Morag Smith
Los Alamos National Laboratory
Los Alamos, NM 87545, USA
505/667-3090

ABSTRACT

The concept of an information barrier, or IB, has been widely discussed for a number of years. An IB is used in a measurement system that contains classified information to prevent the release (either intentional or inadvertent) of the classified information while still allowing an inspecting party to reach independent conclusions as to the contents of a storage container. Typically, an IB would be used in a measurement system regime that requires the owner of certain storage containers to declare the contents of the containers (in unclassified terms) and an inspecting party to confirm this declaration. The IB allows the owner's declaration to be confirmed without releasing any classified information to the inspecting party.

Most IB design concepts are based on two attribute measurement systems (AMSs) that were built and demonstrated in the U.S. in 1999 and 2000. These IBs relied heavily on simple hardware implementations and performed well in a "one-time" demonstration mode. However, implementation of an AMS in a long-term verification regime will place a different set of requirements on the entire AMS system—and the IB, in particular. In this paper, we will concentrate on the effects of changing constraints on IB design, new IB concepts that have been developed since the earlier demonstrations, and design concepts the have been developed within a number of related verification regimes.

INTRODUCTION

The concept of an information barrier (IB) as part of an attribute measurement system (AMS) was first developed within the context of verification measurements for a nuclear material monitoring program [1, 2]. The design goals of the AMS and IB are to protect classified information related to items being monitored while allowing an inspector to remain confident that the results given by the AMS are actually representative of the item being measured. This type of AMS and IB system is currently under development by a team of Russian scientists at the All-Russian Scientific Research Institute of Experimental Physics (VNIIEF) [3, 4]. The measurement system is being developed to measure a number of unclassified "attributes" (such as the presence of plutonium above a certain mass threshold, the degree of enrichment of plutonium, etc.) of potentially classified stored items.

Although the requirements for an IB within an AMS system are perhaps the most stringent in nuclear material verification, there are a number of other areas where the protection of sensitive information must be combined with inspector confidence in the results. Although many systems are available to *either* protect sensitive information *or* enhance inspector confidence [5], a "production-ready" IB concept must address both concerns simultaneously while also maintaining its reliability in an industrial-use environment.

THE INFORMATION BARRIER

The two-state IB, described in more detail in ref. [5], provides both data protection and inspector confidence by enabling both a closed mode (Fig. 1a) for protection of sensitive data and an open mode (Fig. 1b) to enhance inspector confidence.

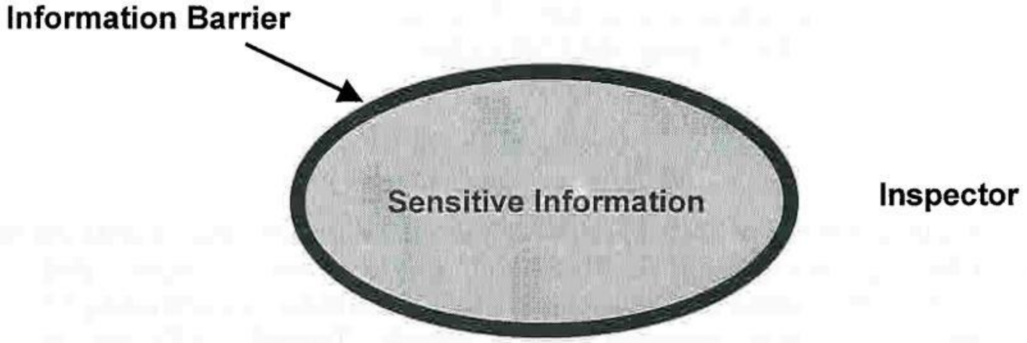


Fig. 1a. Conceptual illustration of an information barrier in the closed mode. All potentially sensitive information is separated physically, electrically, and procedurally from the inspector by the barrier.

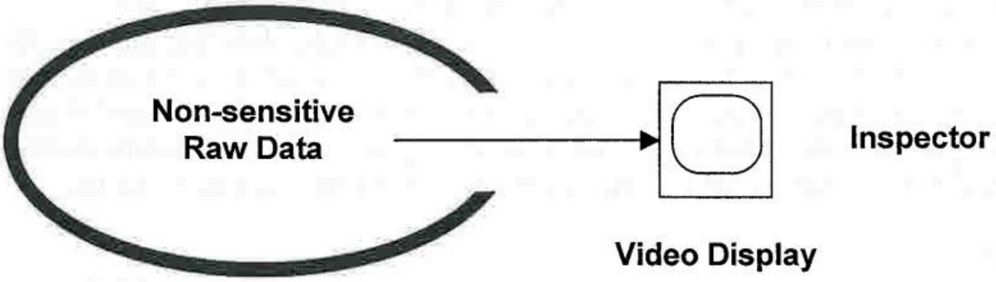


Fig. 1b. An information barrier in the open mode. In this mode, non-sensitive raw data can be displayed on a video monitor as an aid to building confidence in the measurement system. In this mode, an open door in the IB allows the inspector access to the non-sensitive raw data. Procedural and mechanical interlocks prevent the IB from being used in the open mode when sensitive items are being measured.

The Fissile Material Transparency Technology Demonstration (FMTTD) [6] was a technology demonstration that showed how data protection and inspector confidence could be reconciled in a single system. However, this system was not designed with robust field use in mind. The IB technology is still immature and has yet to be realized in a production-ready device. Therefore, each component of the IB is being scrutinized to identify likely failures that may occur during field use. This includes failures in all three design-goal areas of the AMS—data protection, inspector confidence, and mechanical reliability.

MOVING FROM DEMONSTRATION TO FIELD USE

Previous demonstrations of the IB and AMS concepts, such as the FMTTD, have focused largely on the security aspects of an AMS—that is, proving that you could prevent classified information from getting past the IB. As we transition away from demonstration AMS systems and begin to design and build systems intended for field use, we need to take authentication and reliability into account. The FMTTD made only superficial attempts at fostering inspector confidence in the system. Furthermore, it was designed for only a single demonstration and, therefore, no real thought was given to reusability or reliability. As we design the functional components for the next generation IB, we must consider how each design choice affects both the reliability and ease of authentication of the system.

AUTHENTICATION

In this context, authentication refers to instilling confidence in the inspector that the device is performing as intended. The inspector must be confident that the unclassified results seen at the output panel are accurate.

A significant difficulty when building confidence in the AMS is that it contains some very complex hardware and software systems. If the material owner and inspector do not fully understand the inner workings of each component, they will not be confident that there isn't some unknown process occurring "behind the scenes." For this reason, and others, we strongly recommend that all complex hardware and software components of an AMS system be commercial, off-the-shelf (COTS) products. In this way, the inspector and material owner will probably already be familiar with the most complex components. Using existing products also reduces the authentication problem that results from having to examine each schematic and line of code in order to verify that the product being used is the same one they are familiar with. Fortunately, the most complex components of the AMS hardware are likely to be the data acquisition electronics and the data analysis computer, both of which have existing COTS options. Similarly, the most complex pieces of software in an AMS will be the analysis packages—and again, well-understood packages are available.

Of course, COTS components are not available for every module in an AMS—particularly for the IB, which relies largely on custom hardware. Although all of the other hardware and almost all of the software in an AMS can be COTS modules, the IB will probably be composed of entirely custom hardware. Because custom hardware manufactured by the material owner is less likely to instill confidence in the inspector than COTS hardware, it will be prudent to make all custom hardware as simple and easy to authenticate as possible. For these reasons, much of our focus will be on the simplification of the IB itself, to make it easy to authenticate. The goal of the next-generation AMS design is to make all custom hardware and software as simple as possible to further the process of building inspector confidence. A block diagram showing the principal components of a conceptual AMS is shown in Fig. 2. [7]

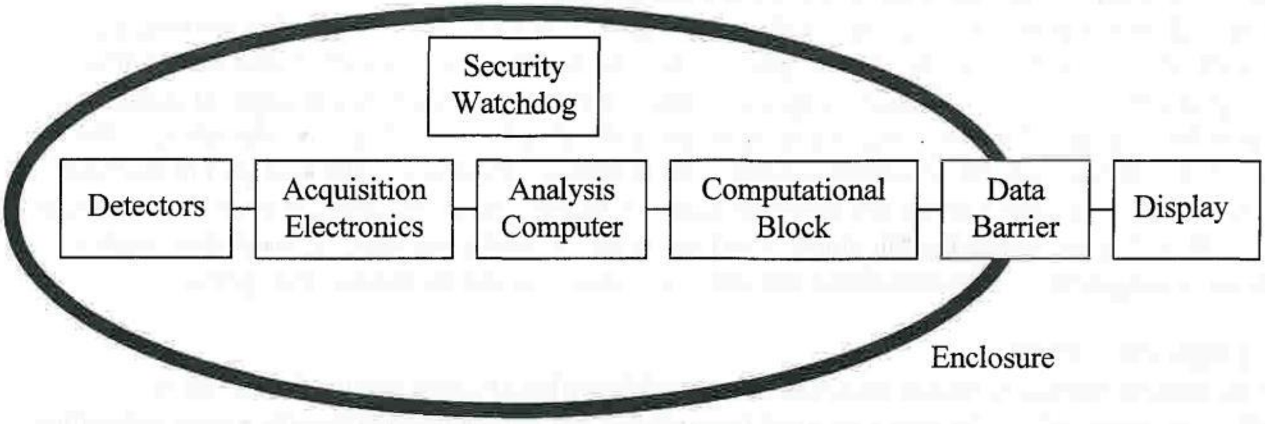


Fig. 2. The modules that make up the information path in an AMS. The security watchdog does not carry data or affect the measurements during normal operating conditions, but it is essential to the security function of the AMS.

Computational Block Authentication
In the FMTTD, the computational block (CB), acting as the main interface between sensitive and non-sensitive information, incorporated a custom-built computer running fairly involved calculations in custom software. The next-generation design reduces this to a single-chip microprocessor [8] running minimal code. The Intel 8051 microprocessor is recommended because it is a well-understood component with an extensive user base. The simplicity of this circuit means that vetting the schematic will be trivial, and the large number of users who are experienced with 8051 circuits means that finding knowledgeable people will also be easy.

Similarly, the functionality of the CB is kept to a bare minimum so its firmware can also be as simple as possible. Serial communication with the analysis computer is handled through hardware, removing the need for large amounts of communication code. The outputs from the CB are a simple function of the state of the control panel inputs and the most recently received messages from the analysis computer. By keeping the firmware simple, an inspector who is reasonably familiar with 8051 operation could quickly determine the functionality of the device by inspecting the source code.

Data Barrier Authentication
The data barrier (DB) module is considerably easier to authenticate than the CB because the DB contains no intelligence. The DB is a passive component designed to be a one-way valve for directing information. The DB on the output lines includes some simple controls that prevent fluctuations in the CB output signal from affecting the displayed results. The DB on the input lines prevents switch bounce or other (possibly malicious) out-of-specification input signals from reaching the CB. The DB has a very simple role and its hardware is correspondingly simple. Someone knowledgeable in electrical engineering can quickly examine the schematic, and the hardware can be checked to see that they match the design.

Security Watchdog and Enclosure Authentication

The security watchdog (SW) is visually separate from the signal processing components of the AMS [6]; all of the security system's sensors and cabling are physically separated from the rest of the AMS. The only commonality between the SW and the rest of the AMS is the fact that the SW controls whether or not the other AMS modules receive power. For this reason, the SW cannot affect the displayed output of the AMS, except by turn it off entirely. Thus, the SW does not have the capacity to reveal sensitive information. However, its function is a critical design criteria for gaining the confidence of the material owner because it is this hardware element that prevents someone from opening the enclosure during an inspection and gaining direct access to the data acquisition electronics or analysis computer, which may contain sensitive data.

The functionality of the SW is simple; it relies on a number of physical switches that monitor the integrity of the hardware enclosures. Authenticating the SW means verifying that these switches are operational and that, when tripped, the SW removes electrical power from all other AMS components. We recommend that the SW include a small display of LEDs to show the current status of each switch. The switches can then be tested quickly; activating a switch would make the corresponding LED on the SW turn off.

Like the DB, the SW contains no real intelligence, and its hardware is extremely simple. A review of the schematic will demonstrate that when any switch is opened, power will be removed from the sensitive AMS modules (when operating in a closed mode).

RELIABILITY

The FMTTD was intended for a single demonstration use in the presence of numerous technicians who were allowed to thoroughly test the system before the demonstration was given. A "production-ready" field unit, on the other hand, will need to be ready to use with little or no intervention. It will be used repeatedly but with long periods of storage between uses. The design of each module, therefore, must be robust, making it capable of operating in a non-controlled industrial environment and able to reliably come back online after long periods of storage.

The most significant design philosophy that supports these goals is modularity. Each component of the AMS is designed around a particular function and is physically separated from the other modules. The startup procedure will include a quick self-check of each module to make sure it is working properly. Any module that is defective can simply be replaced from a pool of spares, rather than troubleshooting in situ. To facilitate this, all custom hardware is designed with low cost as a priority. Thus, having a number of spare replacement modules will be feasible from a cost perspective.

Computational Block Reliability

The CB module has well-defined input and output specifications that do not require exotic hardware to test. A laptop with a serial port and a row of output LEDs could serve as a test bed for a CB module. A procedure for fully testing the functionality of the CB can be developed so that a technician can rapidly verify the working condition of a number of CB boards. The design of the input/output system of the CB is specifically tailored to allow this simple hardware test.

The CB module contains no exotic components and should not degrade in performance after an extended storage period if the environmental conditions of the storage facility are reasonable.

Data Barrier Reliability

The DB, again, is simple, easy to test, and cheap to replace if a problem arises. It is designed with a quick module testing procedure in mind. Also, it contains no components that would degrade during a reasonably long storage period.

Both the DB and the CB are printed circuit boards that are housed in a shielded box that is itself inside the AMS enclosure during storage. Thus they are doubly protected against damage from the environment or mechanical damage from rough handling.

Security Watchdog and Enclosure Reliability

The SW in the FMTTD actually contained moving parts—the reed switches on the doors. In order to ensure the long life of the door switches, the reed switches could be replaced by balanced Hall-effect magnetic switches that have considerable built-in tamper resistance and no moving parts. These switches are designed for the physical security industry, which means they are tailor-made for this application and are also COTS components that can be replaced if necessary.

Because we expect components within the enclosure to be removed periodically for inspection and authentication, the internal wiring should be protected from possible mechanical damage. Putting the door-switch cabling in metal conduit affixed to the inside surfaces of the enclosure will protect it. Because the door-switch wiring is independent of the signal wiring used for the actual measurements, the conduit that contains cabling which might relay sensitive information will be separate from the door-switch wiring conduit.

CONCLUSION

By instituting these design philosophies and directions, we reduce the time required for inspectors and material owners to physically inspect and test the hardware and software operation of the IB components. This means there will be less time and money spent on activities that do not involve actually performing measurements. However, the possibility will always exist that changes have occurred to the hardware, firmware, and software—whether malicious or accidental. These will still have to be examined periodically to verify that everything still works, particularly after being stored for any length of time, the suggestions made here reduce the time and money required for this vetting process. Implementation of these recommendations in the design of an IB will result in a more cost-effective AMS as a whole.

ACKNOWLEDGEMENT

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

REFERENCES

[1] D. W. MacArthur, R. Whiteson, and J. K. Wolford, Jr., "Functional Description of an Information Barrier to Protect Classified Information," Proceedings of the 40th Annual INMM Meeting, Phoenix, AZ, July 25–29, 1999.

[2] D. W. MacArthur and D. G. Langner, "Attribute Verification Systems: Concepts and Status," Proceedings of ESARDA 2003, Stockholm, Sweden, May 13–15, 2003.

[3] J. M. Puckett, D. G. Langner, S.-T. Hsue, D.W. MacArthur, N. J. Nicholas, R. Whiteson, T. B. Gosnell, Z. Koenig, J. Wolford, M. Aparo, J. Kulikov, J. Whichello, V. J. Poplavko, S. F. Razinkov, D. S. Semenov, and V. Terekin, "General Technical Requirements and Functional Specifications for an Attribute Measurement System for the Trilateral Initiative," Proceedings of the 42nd Annual INMM Meeting, Indian Wells, CA, July 15–19, 2001.

[4] Alexander Livke, Tim Elmont, Diana Langner, Duncan MacArthur, Doug Mayo, Morag Smith, Dmitry Budnikov, Mikhail Bulatov, Igor Jarikhine, Alexander Modenov, Anton Morkin, Sergey Razinkov, Sergey Safronov, Dmitry Tsaregorodtsev, Andrey Vlokh, Svetlana Yakovleva, and S. John Luke, "Progress of the AVNG System - Attribute Verification System with Information Barriers for Mass and Isotopics Measurements," to be presented at the INMM 46th Annual Meeting, Phoenix, AZ, July 10–14, 2005.

[5] Duncan W. MacArthur, "Regime-Independent Characteristics of Attribute Measurement Systems," Proceedings of the 44th Annual INMM Meeting, Phoenix, AZ, July 13–17, 2003.

[6] D. W. MacArthur et al., "Attribute Measurement System with Information Barrier for the Fissile Material Transparency Technology Demonstration: System Overview," Los Alamos National Laboratory document LA-UR-99-5611, 1999, Website located at http://www-safeguards.lanl.gov/FMTT/index_main.htm.

[7] J. Shergur et al., "An Overview of the Design of a Next Generation Attribute Measurement System," to be presented at the 46th INMM Annual Meeting, Phoenix, AZ, July 10–14, 2005.

[8] R. Landry et al., "Advantages and Disadvantages of Small Chip Count Device in an Information Barrier," to be presented at the 46th INMM Annual Meeting, Phoenix, AZ, July 10–14, 2005.