LA-UR- 04-4353

Approved for public release; distribution is unlimited.

Title:

INFORMATION BARRIER TECHNOLOGY APPLIED TO LESS RESRICTIVE ENVIRONMENTS

Author(s): D. W. MacArthur , D. G. Langner , and P. A. Hypes

Submitted to: 45th Annual INMM Meeting

Orlando , FL USA
July 18-22, 2004
(INMM Paper)

INFORMATION BARRIER TECHNOLOGY APPLIED TO LESS RESTRICTIVE ENVIRONMENTS

Duncan W. MacArthur, Diana G. Langner and Phil Hypes
Los Alamos National Laboratory
Los Alamos, NM 87545 USA
505/667-8943

ABSTRACT

The information barrier is an important part of any system that allows inspector verification of declared classified materials. In this context, the information barrier must protect classified information while allowing the inspectors to reach correct and independent conclusions concerning the veracity of the declaration. Although other applications may not involve national security, information barrier techniques can still be used to protect information considered sensitive by individuals, commercial entities, or national organizations. Other potential areas of application include homeland security and airport screening, personal information disclosed by modern scanning techniques, nuclear information not considered classified but still sensitive, and industrial secret information that could be compromised during 3rd party acceptance testing. Modern personnel screening devices are limited more by their potential for release of personal information than by technology. Screening systems that could be used in airports and other sensitive areas are often not utilized because the same system that can show the details of weapons carried on a person's body can also reveal potentially embarrassing and sensitive details of the body itself. Much other nuclear information, as well as industrially secret information, while not actually classified, is not appropriate for widespread dissemination. In both cases an inspector may need to verify elements of the manufacturer's or owner's claims, but at the same time not disclose sensitive information to either the inspector or the general public. Thus, information barrier technology, although originally developed for protection of nuclear weapons information, is also directly usable in a number of counter-terrorism and nonproliferation applications. Although these applications may not (or may) require the same level of rigor as the original application to classified items, many of the same techniques can be used in protecting this non-classified, but still sensitive, information.

INTRODUCTION

The concepts of an information barrier (IB) as part of an attribute measurement system (AMS) were first developed to within the context of verification measurements within a nuclear material monitoring regime. [1,2] For this use, the AMS and IB are implemented in such a way as to protect classified information about items being monitored while allowing an inspector to gain confidence that the actual contents of these items are consistent with the declared contents. An AMS and IB system of this type is currently under development by a team of Russian scientists at VNIIEF. [3,4] This measurement system, known as the AVNG, is being developed to measure a number of unclassified "attributes" (presence of plutonium, grade of plutonium, presence of a significant quantity of plutonium) of potentially classified stored items.

Although the nuclear material verification application is perhaps the most stringent, there are a number of other areas where protection of sensitive information must be combined with inspector confidence in the results. Many systems are available to **either** protect sensitive information **or** enhance inspector confidence in these cases; [5] however, a variation of the IB concept addresses both concerns simultaneously.

THE INFORMATION BARRIER

The two-state IB, described in more detail in Ref [5], addresses the two competing concerns (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.

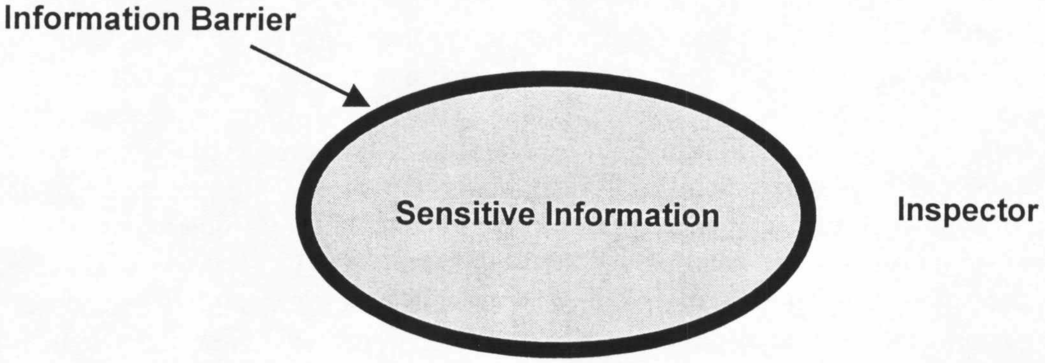

Fig. 1a. Conceptual illustration of an IB in the closed mode. All potentially sensitive information is separated physically, electrically, and procedurally from the inspector by the barrier or series of barriers.

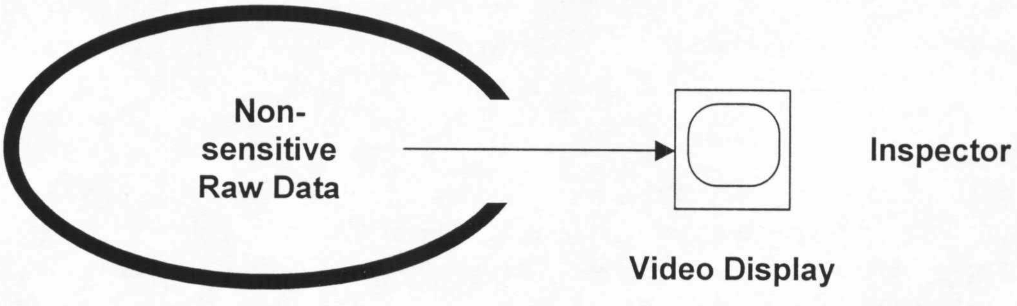

Fig. 1b. An IB in the open mode. In this mode, non-sensitive raw data can be displayed on video monitors as an aid to building confidence in the measurement system. In this mode, an open door in the IB allows the inspector access to the non-sensitive raw data.

“TRADITIONAL” IB USE

An application of these concepts is the AVNG illustrated conceptually in Fig. 2 and described in detail in Refs [4] and [5].

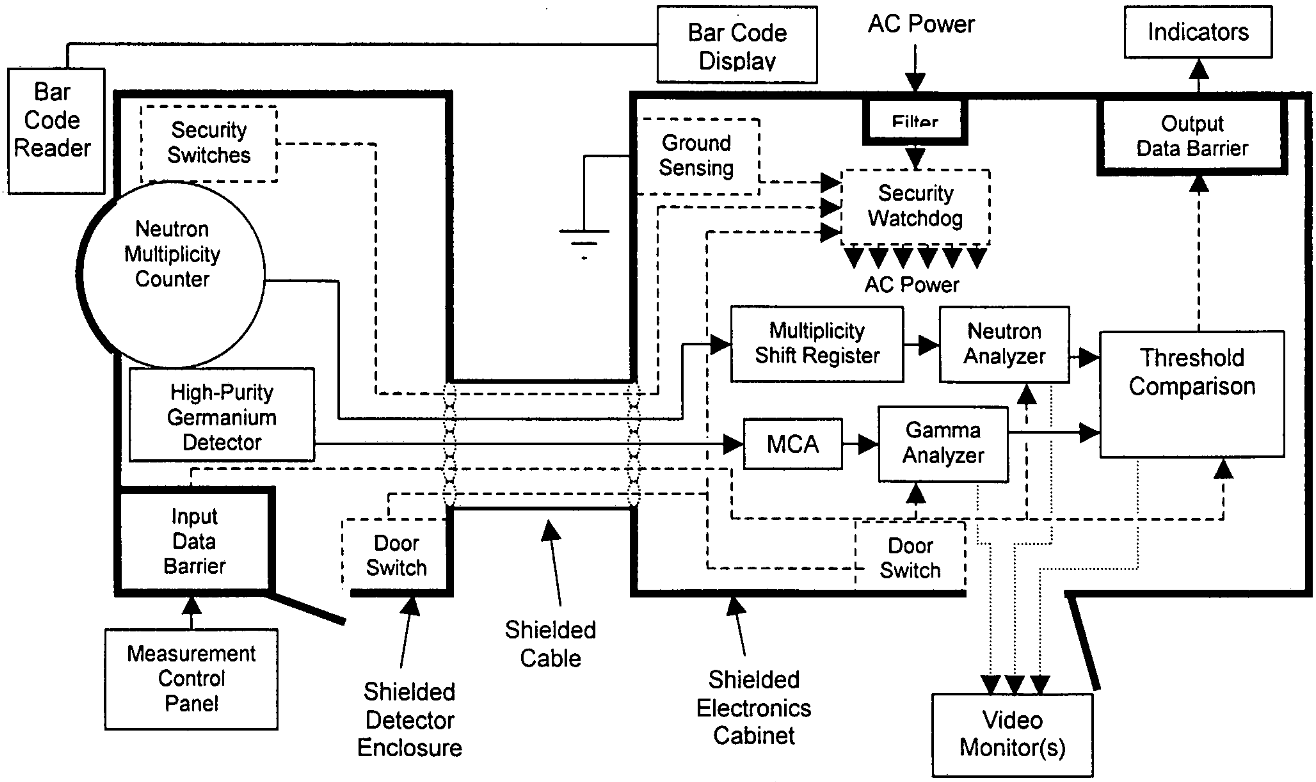

Fig. 2. Conceptual schematic of the AVNG. The complexity shown here is indicative of the difficulties involved with translating the concept of Fig 1 into operational hardware..

In this case, nuclear radiation detectors (High-Resolution Germanium and Neutron Multiplicity Counter) generate the potentially classified raw data. This data is converted into unclassified attribute prior to displace outside of the IB.

PERSONNEL SCREENING AND PERSONAL INFORMATION

Technology for the screening of people to detect illicit objects is more mature than its present application would indicate. A significant obstacle to the application of existing technologies is that in order to have confidence that both metallic and non-metallic items are detected; the imagery must be quite intrusive. Images obtained from a commercial, back-scatter x-ray imaging system clearly identify hidden weapons and illegal drugs hidden under a person’s clothing. However, these images also reveal unacceptable details of the monitored individual’s anatomy. Because such imagery is a clear violation of an individual's right to privacy, such imaging technology is currently only employed when specific legal justification exists. Other sophisticated imaging technologies have similarly not found wide application even though their benefits in combating terrorism and drug trafficking are obvious.

The use of an IB would allow inspectors to draw conclusions about images that contain personal information without revealing any of the sensitive or personal information to the inspector of the public. The IB filters the information and then provides a simple "pass or fail" result to the inspector. If there is any attempt to gain access to the personal information used to make this judgment; the original information is automatically destroyed. Further, with an information barrier system, no images can be saved or archived.

In this case, the IB is made up of a series of hardware, software, and procedural systems to protect personal information while releasing sufficient information to allow an inspector to make a decision concerning contraband substances. The intrusive images are analyzed for "suspicious" objects and a simple display alerts the human inspector to the result without the inspector having the opportunity to examine or archive the images themselves. In order to make this "pass or fail" decision, computerized pattern recognition algorithms would replace the human inspector who would normally perform the visual analysis.

COMMERCIAL INFORMATION AND TESTING

Commercial product testing is another area driven by competing concerns. The manufacturer often considers the exact composition of a product to be proprietary. However, in order to make legitimate advertising claims, the product must be tested and shown to contain more than an established threshold of some particular ingredient. Thus, the issue is to demonstrate that one (or more) ingredient(s) exceeds a given threshold without revealing the exact composition of the product.

Industries could use this technology for product quality control. Regulated food and drug companies would monitor the chemical composition, quality, and safety of their products without revealing their proprietary formulas. A capsule or tablet would be analyzed for required ingredients, using appropriate detectors and analyzing computers in a shielded cabinet and sending the same red/green-light signals outside the cabinet for satisfaction of the U.S. Food and Drug Administration or other regulating agency.

Again, the IB structure (and the non-sensitive nature of the IB hardware) allows the inspectors to have confidence in the threshold results without disclosing any detailed information. The use of such a technical solution would reduce the reliance on human discretion during these measurements.

REMOTE MONITORING

The advantages of the IB in unattended and remote monitoring have been discussed in detail in another paper at this conference. [6] In many cases, unattended and remote monitoring has proven effective in reducing the cost of inspection activities and in reducing the amount of required inspector travel. Remote monitoring methods are also attractive to Host facilities as such methods have the potential for reducing the impact of inspections on the facility. However, if the host country deems that the raw data collected by these systems classified or sensitive, the data cannot be transmitted without further processing.

Remote monitoring of unattended systems can serve several functions:

- Unattended measurement systems can fail; if such a failure is not detected immediately, days or months of safeguards information could be lost before the next site visit. If state-of-health information were remotely transmitted, the impact of such a failure could be reduced or eliminated.
- One of the major impacts of unattended systems is the reduction of number of required site visits. Transmission of the unclassified attribute "comparison with declaration" or similar non-sensitive attributes could reduce the number of physical visits required in an inventory verification regime.
- Data relating to the location of material or items **at the present time** is potentially sensitive. The sensitivities, or classification issues, could often be addressed by introduction of an appropriate transmission delay (similar to that used by radio stations to control the content of their broadcasts).

If the measurement system is exposed to classified data, the host may be reluctant to allow the transmission of any of these types of data because of the potential for unauthorized release of sensitive information. The IB structure can be used to prevent the potential release of classified or sensitive data, build inspector confidence in the veracity of the remotely monitored data, and allow both the inspector and the Host to take advantage of the monetary and procedural benefits of unattended monitoring.

SUMMARY

The IB techniques can be used in any application that requires the protection of sensitive information combined with inspector confidence in the result. This can be restated as any measurement application that requires inspector confidence in data that they (the inspectors) are not allowed to observe directly. A generalized IB concept is shown in Fig. 3. Any attribute for which a suitable measurement system exists can be used within this structure. These measurements can include, but are not limited to, the nuclear, optical, chemical, and mechanical systems discussed here.

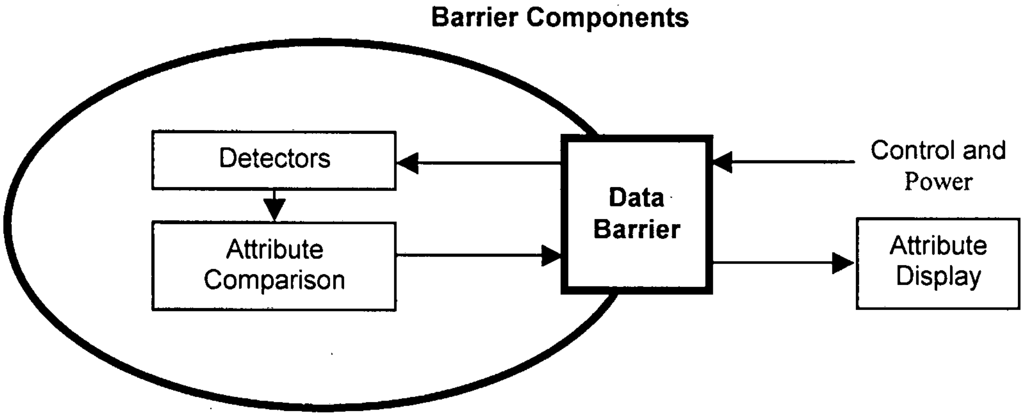

Fig. 3. Generalized implementation of an AMS incorporating an IB. Any attribute for which a suitable measurement technique exists can be used within this structure.

ACKNOWLEDGEMENT

This work is supported by the United States National Nuclear Security Administration's International Safeguards Office.

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 INMM Annual 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 INMM Annual Meeting, Indian Wells, CA, July 15–19, 2001.

[4] A. B. Modenov, B. L. Lebedev, A. V. Livke, , S. F. Razinkov, M. V. Savin, and D. V. Budnikov, "A Physics/Conceptual Design for the AVNG System," Proceedings of the 43rd INMM Annual Meeting, Orlando, FL, June 23–27, 2002.

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

[6] Diana G. Langner and Duncan W. MacArthur, "An Application of Unattended and Remote Monitoring to Sensitive Systems," Presented at the 45th INMM Annual Meeting, Orlando, FL, July 18-22, 2004.