LA-UR- 98-2910

CONF-980733--

Approved for public release; distribution is unlimited.

Title: Use of Information Barriers to Protect Classified Information

Author(s): Duncan MacArthur
M. William Johnson
Nancy Jo Nicholas
Rena Whiteson

Submitted to: Institute of Nuclear Materials Management Conference

July 27-31, 1998
Naples, Florida

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

Use of Information Barriers to Protect Classified Information

Duncan MacArthur, M. William Johnson, Nancy Jo Nicholas, and Rena Whiteson

Los Alamos National Laboratory
Los Alamos, NM 87545

ABSTRACT

This paper discusses the detailed requirements for an information barrier (IB) for use with verification systems that employ intrusive measurement technologies. The IB would protect classified information in a bilateral or multilateral inspection of classified fissile material. Such a barrier must strike a balance between providing the inspecting party the confidence necessary to accept the measurement while protecting the inspected party's classified information. We discuss the structure required of an IB as well as the implications of the IB on detector system maintenance. A "defense-in-depth" approach is proposed which would provide assurance to the inspected party that all sensitive information is protected and to the inspecting party that the measurements are being performed as expected. The barrier could include elements of physical protection (such as locks, surveillance systems, and tamper indicators), hardening of key hardware components, assurance of capabilities and limitations of hardware and software systems, administrative controls, validation and verification of the systems, and error detection and resolution. Finally, an unclassified interface could be used to display and, possibly, record measurement results. The introduction of an IB into an analysis system may result in many otherwise innocuous components (detectors, analyzers, etc.) becoming classified and unavailable for routine maintenance by uncleared personnel. System maintenance and updating will be significantly simplified if the classification status of as many components as possible can be made reversible (i.e. the component can become unclassified following the removal of classified objects).

INTRODUCTION

In this paper we will attempt to define the structure and requirements (both in hardware and software) of an information barrier (IB). We will define an IB as a suite of hardware and software components and procedures that separate a classified data collection system from an unclassified display and user interface. This IB concept[1] will be employed in the radiation measurement instrument(s) used for attribute verification of excess fissile materials offered for international safeguarding.

This paper is specifically not intended as a list of solutions to the problems, but instead, concentrates on generating a thorough discussion of the goals and problems themselves. In some cases we have presented potential solutions; these discussions are meant as illustrations of the types of systems required and are not intended as endorsements of any

particular solution. The simple information barrier concept illustrated in Fig. 1 has been widely discussed. In all figures; dark lines, bold type, and shaded boxes indicate classified areas.

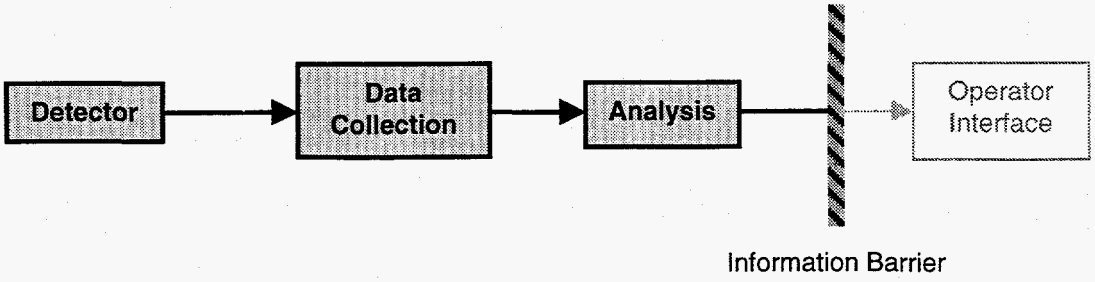

Fig. 1. Simple outline of data acquisition system incorporating an IB. In this figure, everything to the left of the barrier is assumed to be classified while the operator interface is unclassified.

The motivation for information barriers is twofold. The first is to protect the host with a guarantee that no classified measurement data can be disclosed to any inspector or other party. The second is to assure the inspectorate that the unclassified data output is accurate, authentic and useful. To accomplish this purpose it is essential that all parties fully understand the role and limitations of information barriers.

APPROACH TO INFORMATION BARRIERS

An effective approach is to provide a combination of hardware and software barriers, with layers of defense so there is no single-point failure mode. Figure 2 is an extension of Fig. 1 that incorporates many of the potential 'hidden' data paths.

In addition, Fig. 2 includes some of the maintenance paths that will be required in an operational inspection system. All paths crossing the barrier must be considered as potential vulnerabilities; these include the software barrier where the desired data itself crosses the barrier as well as a number of other barrier crossings (mostly requiring hardware barriers) by service connections.

As many elements of the system as possible should be kept on the unclassified side of the IB. This will simplify the difficult task of instilling and maintaining confidence in the IB in all parties. Additionally, unclassified components would be much easier to maintain, service, or replace (if necessary).

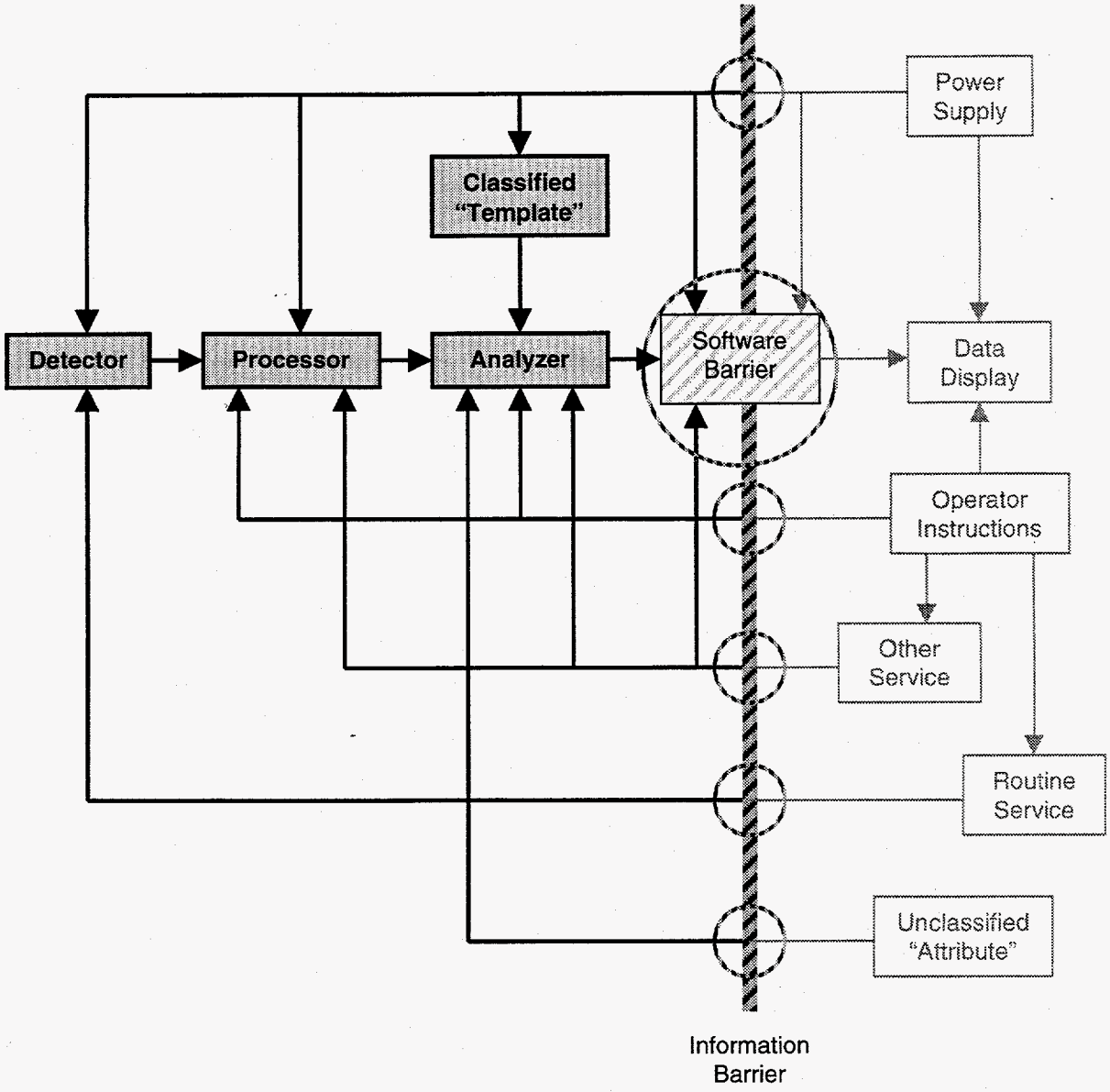

Fig. 2. A more complete diagram of a data acquisition system illustrating both software and hardware components incorporated into the IB. All of the barrier crossings (circled) must be protected. As in Fig. 1, all components to the left of the IB are assumed to be classified; all to the right are unclassified.

Potential layers of protection could include the following elements:

- physical protection, surveillance, and tamper indicators for all hardware,
- hardening of key hardware components,
- assurance of capabilities and limitations of hardware and software systems,
- administrative controls,
- validation and verification of the systems, and
- error detection and resolution.

Physical Protection

Physical protection must be provided for all elements of the inspection system. This may include item such as NDA instruments, computers, network components (if employed), and connectors. Vaults, 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. Hardware components may be hardened with intrinsic protection within chips, cables, etc. In particular, the software (both active and backup copies) and related source files necessary to rebuild the system must be protected in a mutually acceptable fashion.

Hardware Emissions Control

Hardening specific hardware elements in the analyzer system can reduce the potential for clandestine data transmission through 'hidden' IB crossing. These measures could include measures such as:

- power supply filtering,
- radio-frequency emissions suppression, and
- electromagnetic shielding.

Thorough exploration of the topic of hardening is beyond the scope of this paper.

Software Assurance

The software is a very important part of the IB. Key elements include:

- operating system,
- compiler,
- data analyzer,
  - the input will be raw, classified input data from NDA instruments and
  - the output will be analyzed, unclassified data to display
- authentication software to verify that the executable versions of all codes are unchanged since last verified.

In addition to keeping as many of the software components as possible unclassified, the custom written modules should be small and simple and kept to a minimum. Mutually acceptable assurance criteria for all software modules must be written and agreed upon in advance. In order to provide all parties with reliable assurances of the functionality and limitations of the software, some of the following issues need to be addressed:

- Some of the software components will have to be written specifically for this IB. All parties will have to reach agreement on who should write it and what part each party will play in its development.
- All parties should agree upon protocols for assurance measures and verification and validation of software modules.

- Detailed Software Requirements Specifications and Functional Specifications should be written for all custom modules.
- Functional specifications for the software components should detail the assumptions made.
- Requirements and functional specifications should be reviewed and approved by all parties.
- Source code should be reviewed and accepted by all parties.
- All parties should review user's manuals.
- All of the software components should be thoroughly tested and approved by all parties before installation. A testing regimen should be determined and agreeable to all parties.

To protect and tightly control access to the analyzer, the IB and other software, protective measures such as the following should be employed:

- An access control system, such as encryption and digital signatures, could be used to control access to all modules for which it is agreed appropriate.
- Development of the software systems should be done with a goal of eliminating or minimizing data retained between inspections. Ideally, only unclassified data will be stored. If classified data must be saved, it may require encryption as well as physical protection.
- All software, including the operating system, will probably require software protection, such as two person logins with passwords and/or decryption keys (one from host, one from inspector). After commissioning, logins will probably be strictly controlled.
- Authorizations for users should limit which functions may be performed and under what conditions.
- Software systems which will automatically logout users after a period of inactivity.
- Software maintenance should be done under strict conditions and observed by all parties.

Administrative Controls

Administrative control may be accomplished through the use of a detailed procedural rulebook for behavior of all participants during inspections, during routine maintenance, and at other times considered necessary. An activity log could be maintained to provide continuity of knowledge. Representatives from all parties will be welcome to participate in all stages of development and installation of system elements. Levels of participation must be agreed upon in advance by all parties. Such participation may be desired for activities such as:

- installation of hardware components,
- set-up of physical protection systems,
- installation of operating system and all software modules, and
- installation and compilation of data analyzer and authentication software.

It will be determined and agreed upon by all parties as to which hardware and software components will be accessed by keys, passwords, or similar methods as well as what type of system will be used.

Administrative control will also be required in order to maintain operational security. The best information barrier system imaginable will be useless if any of the parties are 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 which record personal dose or dose rate).

Validation and Verification

At the time of an inspection, the system checks by all relevant parties may include:

- examination of the physical protection of all hardware and software system elements,
- testing of analysis system on non-classified sources,
- authentication of analyzer, system, and data collection software and verification of the lack of changes, and
- authentication of data stored (if any) from previous inspections.

Error Detection & Resolution

Two types of errors can occur during operation of the inspection system. System errors would involve the failure of one or more elements of the analysis system; possibly in a subtle fashion. Measurement errors would result in the system misidentifying the device under test. System errors must be detectable and rectifiable without revealing classified information. Many of these problems are similar to the maintenance issues discussed below.

It would be ideal if the analyzer software were able to detect erroneous output (measurement errors) and determine the correct output for given input. However, it may not be achievable. Error detection is a hard problem in the best circumstances. If the output of the analyzer is binary, i.e. YES or NO, once an error is detected, correction will be trivial. If the output is more diverse, resolution will be extremely difficult.

Either type of error can cause either false negative or false positive results. Very simplistically, the inspected party would seem to desire few (if any) false negatives without worrying much about the incidence of false positives. The desires of the inspectorate would seem to be exactly opposite, much more concerned with the incidence of false positive responses. Both error rates can be determined for a given analysis system. It is essential that all parties agree to a single set of acceptable error rates so that all results are directly comparable.

Error checking circuitry can create an additional barrier crossing which must be protected. Any control signal (such as an error message) which passes from the unclassified to the classified area has the potential for carrying information in the other direction.

MAINTENANCE ISSUES

In any real system, maintenance will be required on a routine basis, and it will be necessary to find a way for this to be done without compromising any party's confidence in the system. Over time, it may become necessary to upgrade commercial or custom hardware and software modules. Protocols will need to be developed and strictly followed. As stated earlier, components in the unclassified area will be much easier to maintain.

One problem associated with simple IB concepts is illustrated in Figs. 3, 4, and 5. Prior to any operation involving 'real' test objects, the entire analysis system is unclassified; all parties can verify that the system works correctly and as claimed. This mode of operation is illustrated in Fig. 3.

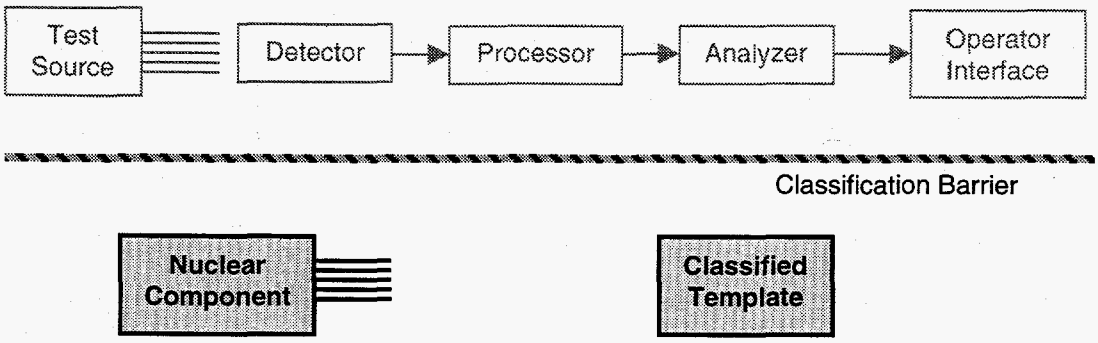

Fig. 3. Analysis system prior to introduction of any classified material. The classification barrier protects all sensitive items. The entire analysis system is functional and can be tested and verified by all parties. All components below the classification barrier are protected by classification.

After all parties are satisfied with the performance of the system, the unclassified test source is removed and the actual devices to be monitored and any classified template are introduced into the system. This stage is illustrated schematically in Fig. 4.

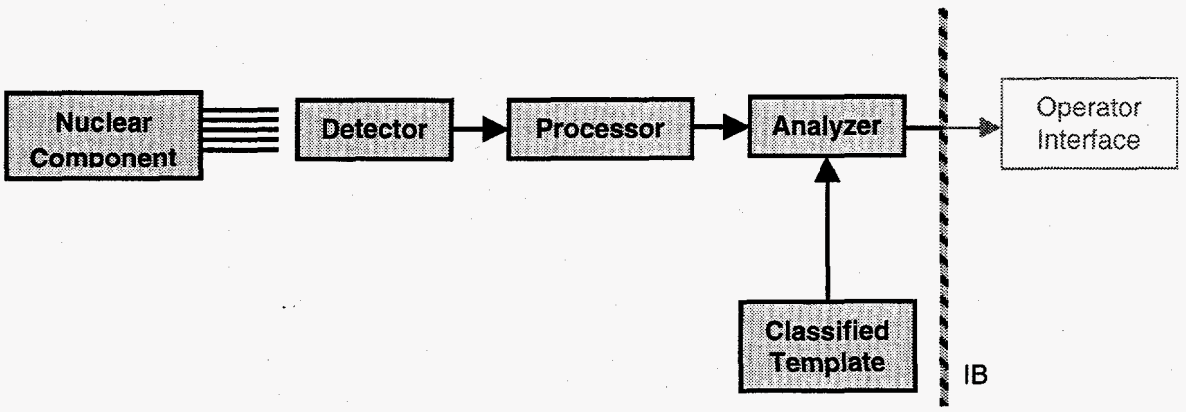

Fig. 4. Analysis system after the introduction of classified nuclear material. The IB now protects the sensitive items and data. At this time, the detector and analysis system are not available for inspection. All components to the left of the IB are assumed to be classified.

Up to this point, the simple model has functioned well. When maintenance is required the nuclear device and classified template will be removed. Unfortunately, as illustrated in Fig. 5, the IB will still be in place, "protecting" the detector, processor, and analyzer.

Since the detector, processor, and analyzer remain in a protected area, maintenance of these items will require strict control. In particular, manufacturer's representatives will probably not be allowed to work on these systems. The mode of operation illustrated in Figs. 3 – 5 can be termed irreversible, i.e. once the system has been exposed to classified material, the entire system becomes classified and will remain that way even when the original classified material is removed.

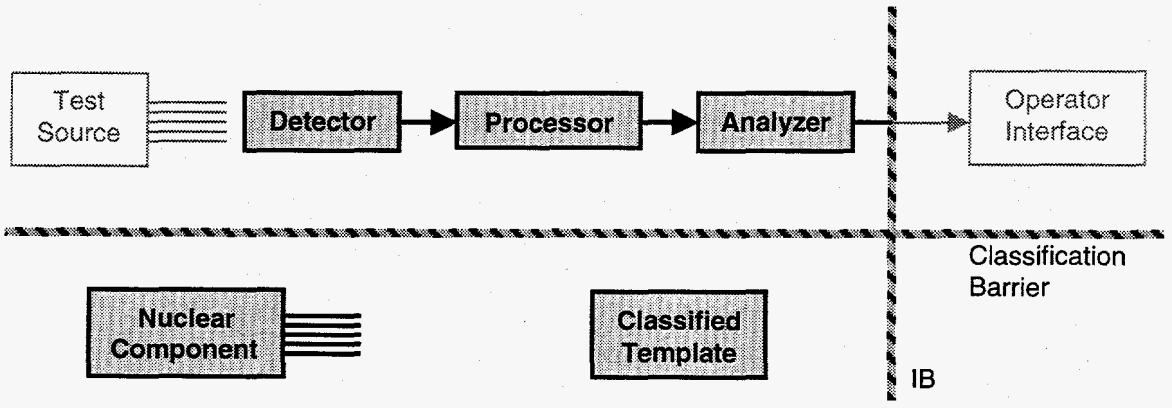

Fig. 5. Maintenance mode – Although all classified material has been removed from the analysis system, the detector, processor, and analyzer remain inaccessible due to the IB. Dark lines, bold type, and shaded boxes indicate classified components.

CONCLUSIONS

A successful IB requires elements of physical, hardware, software, and administrative control. Understanding the interplay between the various components is essential. It is critical that the software and hardware components not be developed independently. Detailed declaration must be made to all parties of the capabilities and limitations of all the hardware and software systems. All parties must be comfortable with the system of technical and administrative controls and their implementation.

A reversible system would facilitate maintenance as well as ongoing system verification and testing. In a completely reversible system, the maintenance mode (analogous to Fig. 5) would be identical to Fig. 3. In this case, all components that were unclassified prior to insertion of classified material would revert to unclassified status following the removal of the material. It is not clear that a completely reversible system is possible in a trilateral inspection system. However, as many components as possible should be made reversible.

ACKNOWLEDGEMENTS

We would like to acknowledge the contributions of Bryan Fearey, William Hunteman, , Joan Prommel, Doug Smathers, Brian Smith, Keith Tolk, and James Tape to this paper. This work was supported by the USDOE.

REFERENCES

1. Whiteson, R and MacArthur, D.W., "Information Barriers in the Trilateral Initiative: Conceptual Description," Los Alamos National Laboratory Report LAUR-98-2137, June 1998.