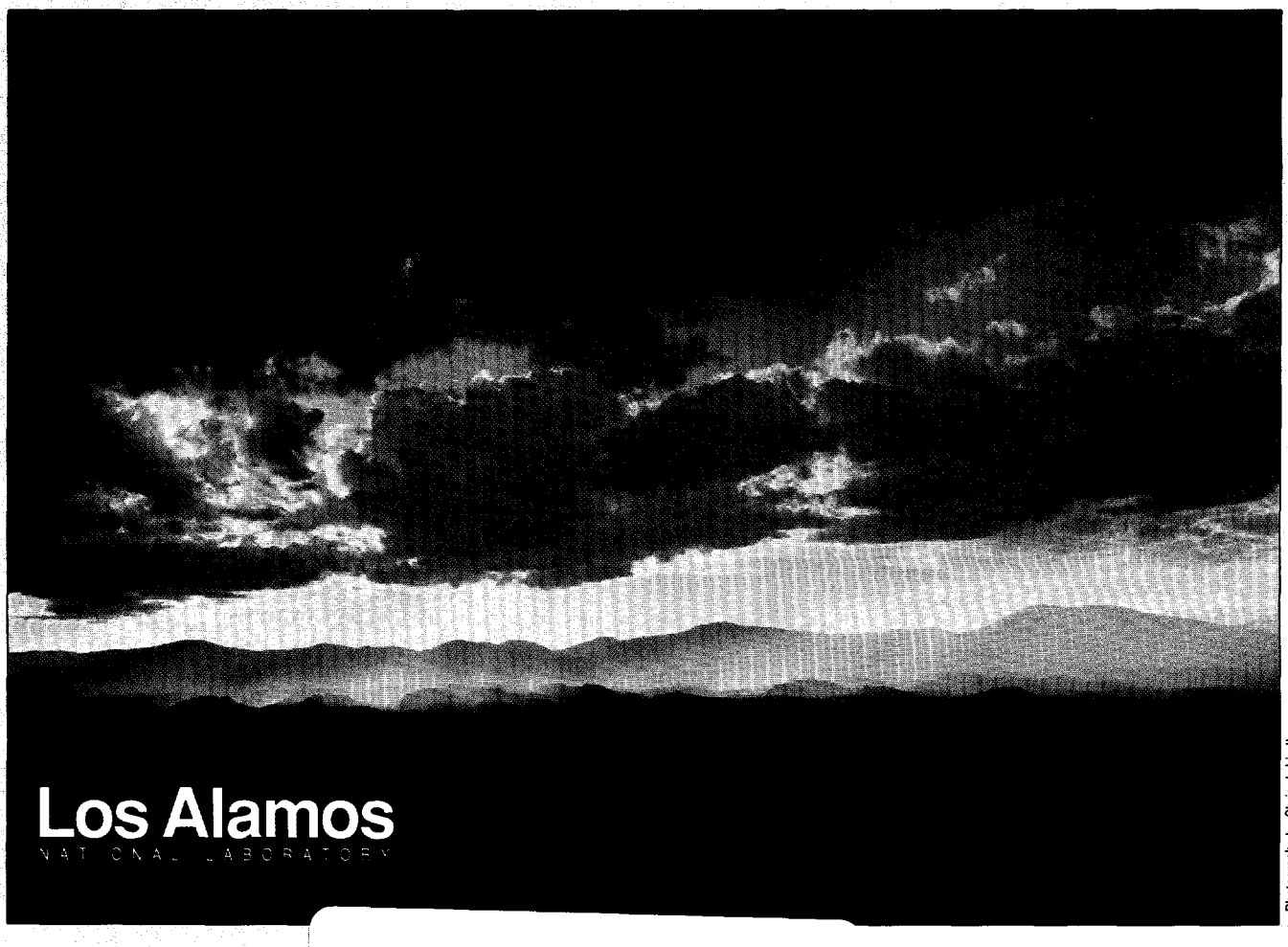
LAUR-98-2137

Information Barriers In the Trilateral Initiative: Conceptual Description

R. Whiteson and D.W. MacArthur
Los Alamos National Laboratory
1998



Photograph: by Chris J. Lindberg

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Table of Contents

Table of Contents 2
1.0 Introduction 3
2.0 Definition 3
3.0 Goal 3
4.0 Approach 4
4.1 Physical Protection 5
4.2 Hardware Emissions Control 6
4.3 Software Assurance 6
4.4 Administrative Controls 7
4.5 Validation and Verification 8
4.6 Error Detection & Resolution 8
5.0 Maintenance 9
6.0 Construction 11
7.0 Challenges 11
8.0 Acknowledgements 11
9.0 Appendix – Color Figures 12

1.0 Introduction

In this paper we will attempt to define the structure and requirements (both in hardware and software) of an information barrier (IB) for the trilateral initiative. This IB concept will be employed in the radiation measurement instrument(s) used for attribute verification of excess fissile materials offered for international safeguarding. In this paper, we will specifically not attempt to present a list of solutions to the problems, but instead, concentrate 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.

2.0 Definition

Information Barrier– A suite of hardware and software components and procedures which separate a classified data layer and an unclassified display layer. The goal of the information barrier is to guarantee that only agreed upon unclassified data is displayed. The information barrier concept illustrated in Fig. 1 has been widely discussed, both in the US and in Russia.

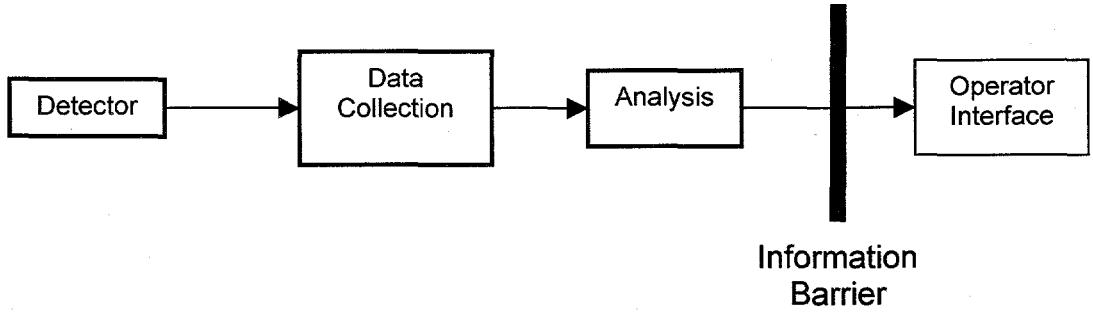


Fig. 1. Simple outline of data acquisition system incorporating an IB. In this figure, everything to the left of the barrier is assumed to be classified while the operator interface is unclassified. (see color figure appendix)

3.0 Goal

The motivation for information barriers is twofold. The first is to protect the host with a guarantee that no classified measurement data can be shared with any inspector. 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.

4.0 Approach

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 which incorporates many of the potential 'hidden' data paths.

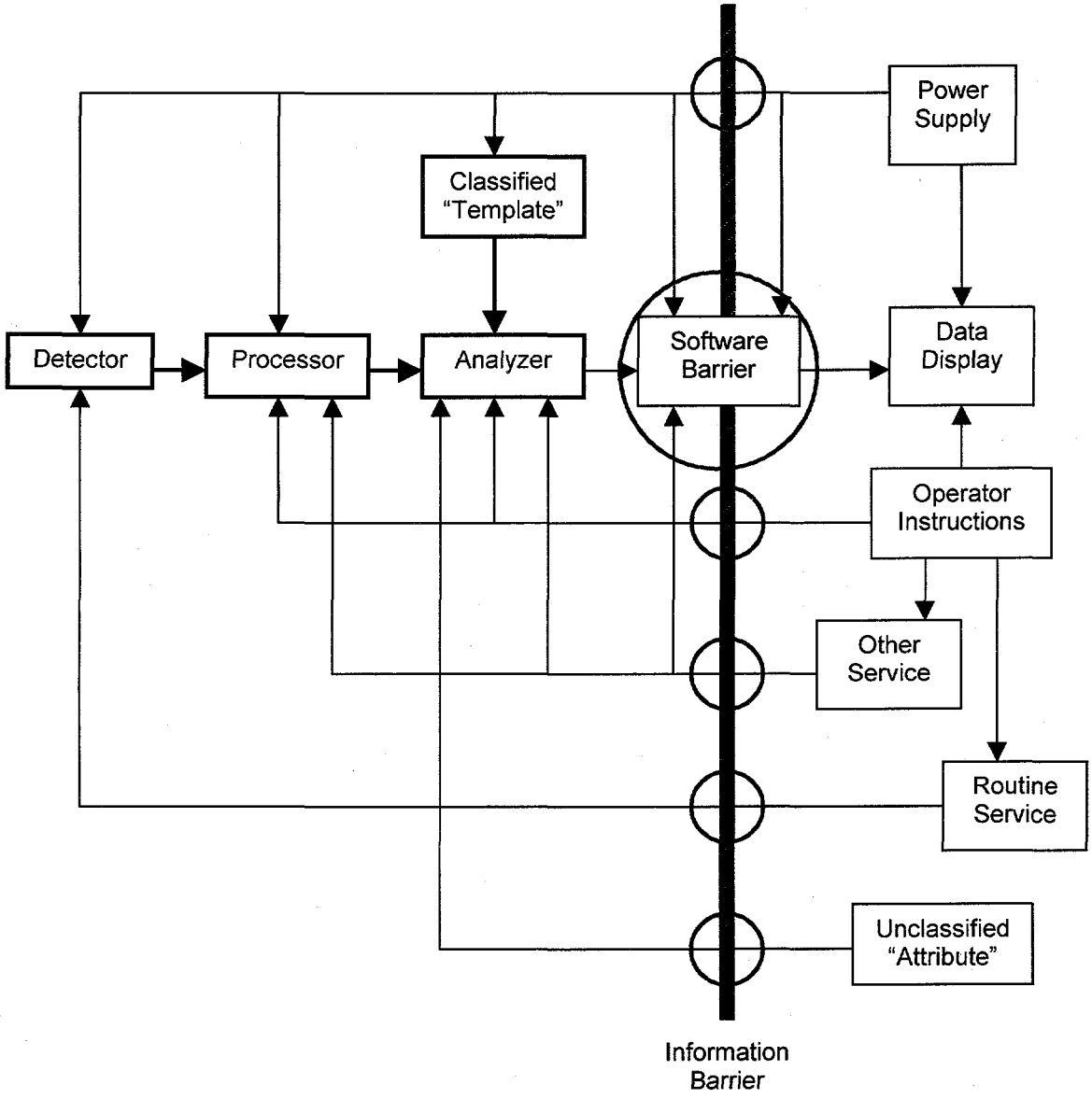


Fig. 2. A more complete diagram of a data acquisition system illustrating both software and hardware components incorporated into the IB. All of the barrier crossings (circled) must be protected. As in Fig. 1, all components to the left of the IB are assumed to be classified; all to the right are unclassified.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

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 components 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).

Potential layers of protection could include the following components:

- physical protection, surveillance, and tamper indicators for all hardware (section 4.1),
- hardening of key hardware components (section 4.2),
- assurance of capabilities and limitations of hardware and software systems (section 4.3),
- administrative controls (section 4.4),
- validation and verification of the systems (section 4.5), and
- error detection and resolution (section 4.6).

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.

4.1 Physical Protection

Physical protection must be provided for all components 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.

4.2 Hardware Emissions Control

The potential for clandestine data transmission through 'hidden' IB crossing can be reduced by hardening specific hardware elements in the analyzer system. 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.

4.3 Software Assurance

The software is a very important element of the IB. Key components 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 above 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 other parties will play in its development.
- Protocols for assurance measures, and verification and validation of software modules should be agreed upon by all parties.
- 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.
- User's manuals should be reviewed by all parties.
- 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.

Note: There are export controls that may prevent the export of certain encryption codes, however, other,potentially acceptable codes are available .

4.4 Administrative Controls

Additional protections can be provided administratively. This may be accomplished with 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 components. Levels of participation must be agreed upon in advance by all parties. 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).

4.5 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 components,
- 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.

4.6 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 components 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 in section 5.

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 be 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.

5.0 Maintenance

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 as step 1 shown in Fig. 3.

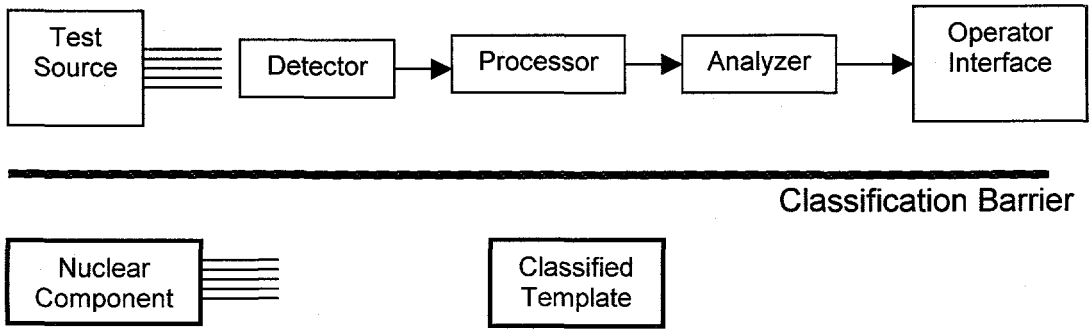


Fig. 3. Step 1 - Analysis system prior to introduction of any classified material. All sensitive items are protected by the classification barrier. The entire analysis system is functional and can be tested and verified by all parties. (see color figure appendix)

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 as step 2 shown in Fig. 4.

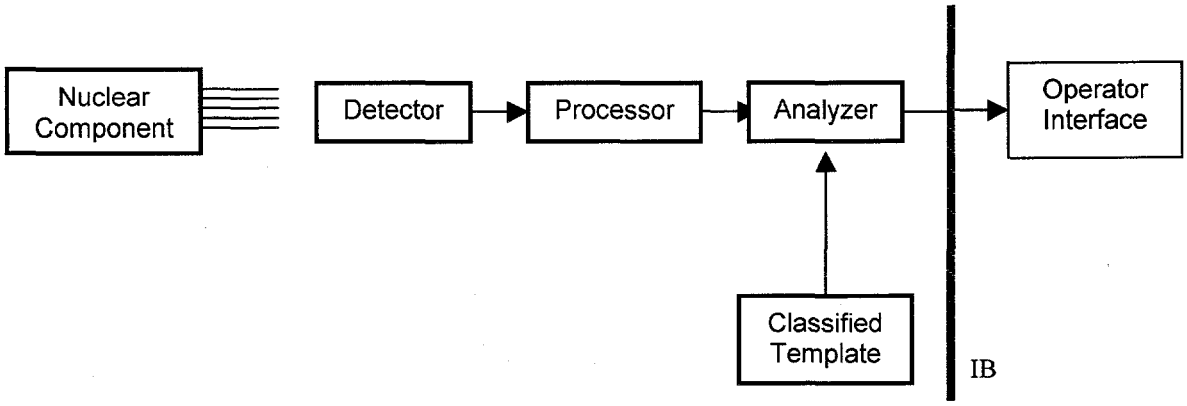


Fig. 4. Step 2 – Analysis system after the introduction of classified nuclear material. The sensitive items are now protected by the IB. At this time, the detector and analysis system are not available for inspection. (see color figure appendix)

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 and analyzer.

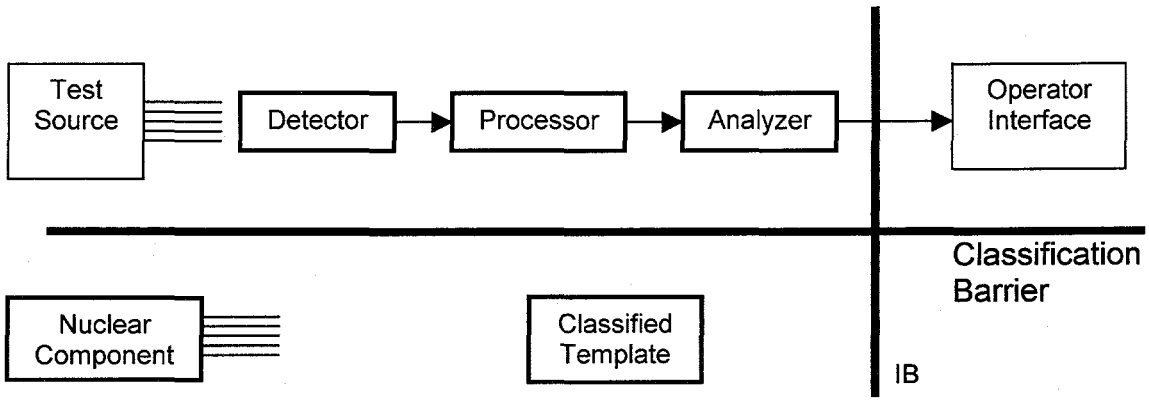


Fig. 5. Maintenance mode – All classified material has been removed from the analysis system, but both the detector and analyzer remain inaccessible. (see color figure appendix)

Since the detector and analyzer remain in a protected area, maintenance of these items will require strict control. In particular, manufacturers representatives will probably not be able to work on these systems. The mode of operation described 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.

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 which 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 this case. However, as many components as possible should be reversible.

6.0 Construction

For a variety of reasons, including maintenance, reliability, ease of upgrades, and long effective lifetime, commercially available components (both hardware and software) are preferable for the system construction. Obviously, some components (for example classified templates) will probably have to be custom designs. However, as many components as possible should not be custom designs. If these components, in addition to being commercially available, are operated in a reversible (i.e. the component can be returned to an unclassified condition after taking classified data) manner, then commercial expertise could be utilized when maintenance or upgrading is required.

7.0 Challenges

In developing an IB that is effective, reliable, and acceptable to all parties, difficult challenges must be addressed. These include, but are not limited to:

- performing comprehensive risk analysis including probabilities of occurrence and impact,
- preparing detailed protocols for response to anomalous situations,
- detection and correction of inadvertent operator errors,
- detection of failed attempts at tampering or misuse,
- detection and handling of successful intrusions,
- methods for resolution of conflicts between parties,
- protocols for recovery from power outages or system failures, and
- methodologies for source code review and acceptance.

8.0 Acknowledgements

We would like to acknowledge the contributions of Bryan Fearey, William Hunteman, M. William Johnson, Nancy Jo Nicholas, Joan Prommel, Doug Smathers, Brian Smith, Keith Tolk, and James Tape to this document.

9.0 Appendix – Color Figures

All of the figures were originally created in color using green boxes and text for unclassified items, red boxes and text for classified items, and red & green striped lines for barriers. To facilitate reading of black and white copies, the borders on the classified (red) boxes have been made thicker than the unclassified ones. In addition, the red items print as black and the green as a gray.