Building a Dedicated Information Barrier System for Warhead and Sensitive Item Verification*

Peter B. Zuhoski, Joseph P. Indusi, and Peter E. Vanier
Brookhaven National Laboratory
Building 197C, P.O. Box 5000 Upton, NY 11973 516/344-4742 FAX: 510/344-1427

Abstract

This paper documents the development of a dedicated information barrier system for warhead and sensitive item verification. The system we describe includes software and hardware information barriers used in conjunction with suitable procedures (or protocols) to achieve a high quality verification while minimizing intrusiveness and preventing transfer of sensitive data to inspectors. The system we describe has been referred to as CIVET – Controlled Intrusiveness Verification Technology and has been implemented to verify warheads and warhead components during various exercises and demonstrations under the auspices of the Department of Energy (DOE) and the Department of Defense (DOD).

Introduction

The concept of CIVET, or in more current terminology a "hardware/software information barrier," was first conceived in 1988 by J. Sanborn of BNL and published in 1991.[1] The concept was pursued under DOE Office of Research and Development (NN-20) funding for several years with early work demonstrating the feasibility of using simple computer systems connected to high resolution detectors to verify by software analysis the validity of sensitive treaty items while limiting the output to the inspector to a simple go/no-go result. In its current configuration the CIVET systems utilize a high-resolution gamma spectrometer (HRGS) as the sensing or detector system. The CIVET HRGS system was tested in field trials in 1994 and successfully demonstrated its ability to verify sensitive treaty items. A feasibility assessment confirmed its utility in verifying sensitive items.[2] In recent experiments in 1997 and 1998, the HRGS system has proven to be a very powerful technique for verifying nuclear warheads and matching SNM bearing components to full-up warheads of the same type.

The CIVET concept recognized the inherent conflict between the inspecting party which desires to carry out a high quality verification and the inspected party which desires to limit the intrusiveness and potential transfer of sensitive data to the inspecting party. In the CIVET concept, data from high-resolution detectors is analyzed by jointly developed software on a simple verifiable computer system (also jointly developed) to reach verification or transparency conclusions. Hence, the CIVET system has built-in intelligence (jointly developed software) to draw reliable verification conclusions from intrusive data without revealing sensitive data to inspectors. To gain additional assurance, the CIVET hardware can accept data input from a variety of sensors and process these to give meaningful but non-sensitive conclusions. Other sensor technologies with possible application include radiographic imaging, gross neutron emission and thermal neutron imaging. The collective hardware, software and procedures constitute a complete information barrier system to assure high quality verification while minimizing intrusiveness and the transfer of sensitive data.

*This work was sponsored by the U.S. Department of Energy under Contract No. DE-AC02-98CH10886.

Alternative approaches or information barrier concepts have been proposed to deal with the problem of verifying sensitive treaty limited items. One approach proposed elsewhere was to utilize low-resolution detectors which would provide some assurance while minimizing intrusiveness. This approach, however, offers limited assurance and is vulnerable to spoofing. Other information barrier approaches propose to utilize commercially available hardware[3] with special procedures and protocols. Because the CIVET system utilizes hardware and software tailored to the specific treaty limited item, it is referred to as a "dedicated" information barrier system.

The remainder of this paper will focus on the software and hardware design principles of the CIVET system and will not discuss the HRGS system and test results except where needed to illustrate the software design principles. We also do not discuss custody protocols, measurement procedures, etc., but focus on the hardware and software information barrier concepts.

The CIVET System

Since the CIVET concept was first proposed, considerable thought and effort went into the design of the system. The major guiding principles used to design the CIVET dedicated information barrier system were the following:

1. The system must be unable to transmit data.
2. The system must be unable to covertly store data.
3. The system must assure proper program (software) execution.
4. The system must verify proper sensor operation.
5. The system must securely protect collected data.
6. The system must be composed of exportable technology.
7. Both hardware and software must be inspectable.

The approach taken in the design of the CIVET information barrier system was to design a dedicated total system because of the difficulties encountered in authenticating commercial off-the-shelf computers that may constitute part of the system. Among the problems encountered with commercial laptop computers were:

- Lack of documentation – Comprehensive documentation for most systems was difficult or impossible to obtain, because proprietary designs are used.
- Laptops are difficult to disassemble and contain specialized/optimized components, which are difficult to verify because of encapsulation.
- Binary Input-Output Systems (BIOS) have become complex – Validating BIOS and operating software would be a significant burden.
- BIOS is stored in EEPROM and can be reconfigured by software.
- New plug and play devices have to provide for auto execution during power on.
- The use of several large and unique application specific integrated circuits – Inspection procedures for validating LSI components would be extremely costly.
- Many I/O devices needed for operation, which increase the complexity of these systems and make verification difficult.

Even in relatively common computer systems, verifying hardware can be problematic unless the design is simple and utilizes well-documented components. For example, a three-pin serial storage device could be mistaken for a transistor.

Based on the seven guiding principles listed above, consideration of the difficulties encountered in verifying commercial computers, and other issues, the CIVET information barrier design is characterized by the following considerations:

1. The CIVET information barrier system is a total system design dedicated to the verification of sensitive treaty limited items.
2. Only MIL SPEC components are utilized in the hardware portion of the system.
3. The variation in types of hardware components is minimized.
4. Software for the system is source code developed specifically for the application.
5. The application program is the only software for the system – there is no operating system.
6. All data and the application program reside on PCMCIA Cards, which can be controlled by appropriate procedures – there are no disk drives or other nonvolatile storage devices.
7. Hardware features may only be added if they improve system security.
8. Full documentation is provided for all levels of the system, down to the mask patterns of integrated circuits.

The documentation of the system and its components provides the basis for verifying the operation of the system and validating the hardware configuration. At the system level the documentation includes the family tree, parts list, assembly diagrams, mechanical drawings, wiring harness drawings, and circuit descriptions. Card level documentation includes schematics, parts list, assembly diagrams, mechanical drawings, theory of operation, diagnostic tests, trouble shooting guidance, and as built photographs. At the chip level, the documentation includes electrical specifications, mechanical specifications, die metallization photographs, test vectors and diagnostic data.

The design of the CIVET dedicated information barrier system also incorporates a number of checking or safeguard features that provide additional assistance to both parties. These include:

1. The applications program is checked by both hardware and software systems for errors, changes, corruption or other defects.
2. The application software configures the input and output circuits.
3. The hardware and software systems encrypt the data.

The CIVET configuration is shown in the CIVET BLOCK DIAGRAM, Figure 1.

PCMCIA cards are utilized for the Error Detection Code ROM, the Application Program Code ROM, the Inspector Security Data (one time programmable memory), the Inspector Data, and the Application Work Memory (random access memory). Figure 1 also shows the address, data and control busses as well as the CPU. The analog-to-digital converter, amplifier, gamma detector, and high voltage power supply in the lower right hand corner are not part of the CIVET hardware and software information barrier system but are shown to illustrate the use of CIVET with the HRGS detector.

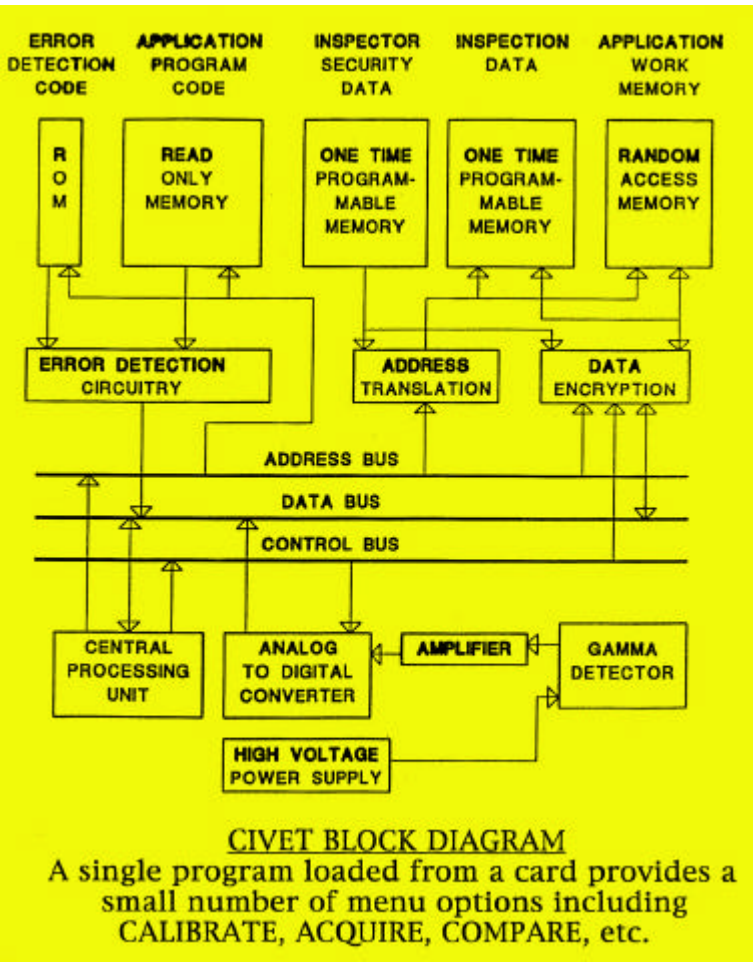

Figure 1. CIVET Block Diagram

The CIVET design supports a number of capabilities needed in testing and assuring the proper functioning of an information barrier system. Among these are:

Authenticating Program Execution: Program execution is assured by several checks involving both the software and hardware systems. The hardware configuration is checked by an 8-bit error correction code. The software generates several checksums for each area of the program specified by the inspecting party. In addition, during startup, a CPU instruction diagnostic is run.

System Performance Verification: This is assured by several mechanisms, including the use of a check source or known test object. The computer system is checked by running a diagnostic using built-in test features, such as reference voltages check and a pulser check.

Data Security Measures: To assure security of the input data, several capabilities are provided. First, the inspecting party's security card loads Field Programmable Gate Arrays (FPGAs) to routes address lines and data lines to random access memory and the template card to

prevent reading of the pre-stored data or code. The term “template” refers to the data acquired from a known authentic treaty limited item of a given type. This “template” data is used to compare data from other items of the same type or to correlate components from dismantlement of a full-up weapon or complete treaty limited item. There is also a provision for additional hardware data encryption by logic from the inspecting party security card and this may consist of look-up tables and functions of the address of the data. In addition, there is software encryption of the data by a key provided by the operator of the system. The operator of the system is generally the host state representative or the inspected party.

Validation of Discrete Hardware Components: To validate elements of the hardware system, there are a number of procedures that are made possible and cost effective by the special simple and dedicated design of the hardware system. Such activities would be extremely expensive and time consuming, if not impossible, for much of the commercial computer equipment available today. For discrete components such as capacitors, transistors, diodes, etc., it is possible to conduct functional tests, measure relevant parameters, and destructively test items on a random sample basis. Microphotography of the boards and X-raying of certain devices has shown to be effective in detecting changes to components or circuits (see Figure 2).

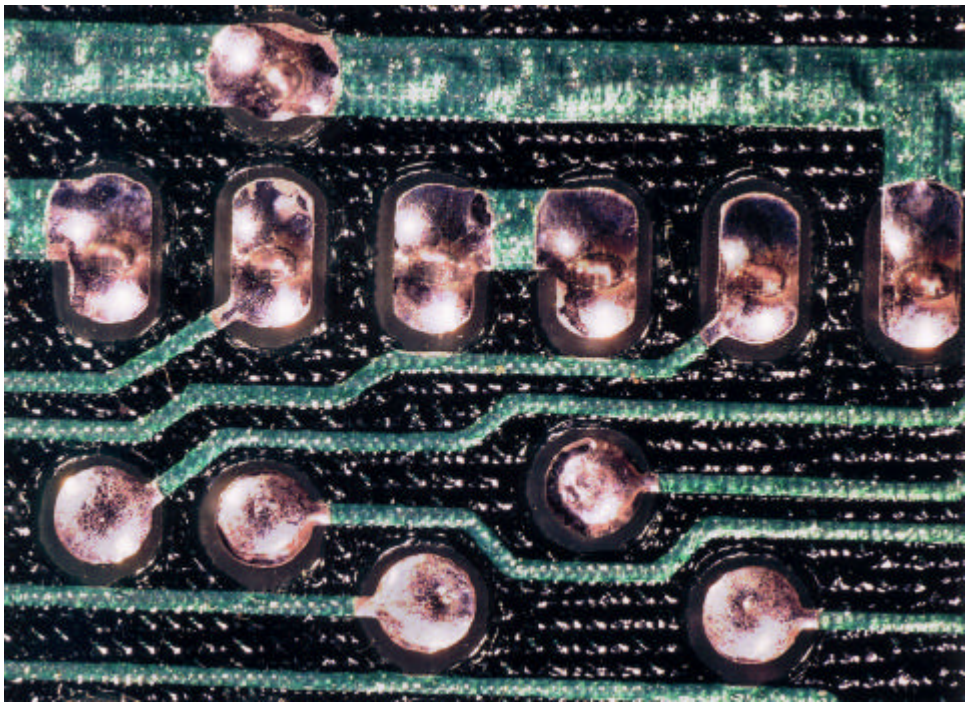

Figure 2. View of Portion of CIVET Mother Board

Validation of Programmable Logic Devices (PLDs): The validation of PLDs used in the hardware system is possible through several relatively simple procedures. Again, this is made possible and cost-effective by the simple design of the CIVET hardware system. For example, serial numbers may be assigned to all PLDs and microphotographs can be made through the window of each device. Each device is programmed with test logic, test vectors may then be run, then the device is programmed with the final logic, test vectors are run again, and the device is then installed in the system. Diagnostic tests are then run on the device as installed.

Validation of FPGA Parts: To validate FPGAs, the following verification activities may be undertaken. The dye is packaged in a window carrier for ease of inspection. The device is then configured with test functions and then test vectors are run to verify functionality. The device is then configured with the final logic followed by test vector runs. In addition, the dye metallization can be micro-photographed and then compared to the chip in the circuit.

Validation of the CPU: The CPU may be validated by several means. First, the CPU may be obtained by a random sampling scheme from many items of the desired type. The lid may be removed to expose the die and this may be compared to a microphotograph of the metallization for the device selected. Finally, a diagnostic may be run in a test configuration to assure proper functionality.

A photograph of the actual CIVET hardware is shown in Figure 3. Figure 4 shows the CIVET information barrier hardware system on the right side with the HRGS system components connected to the input. There are two CIVET systems in existence and the configuration shown in Figure 4 was the system used in field trials to successfully verify complete treaty-limited items.

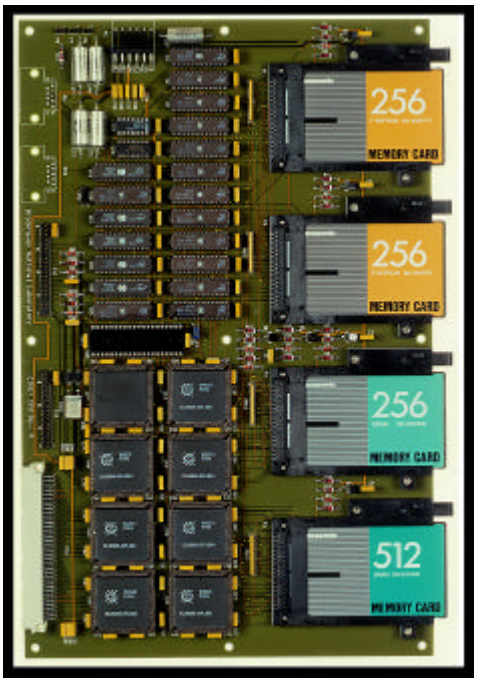

Figure 3. CIVET Hardware System

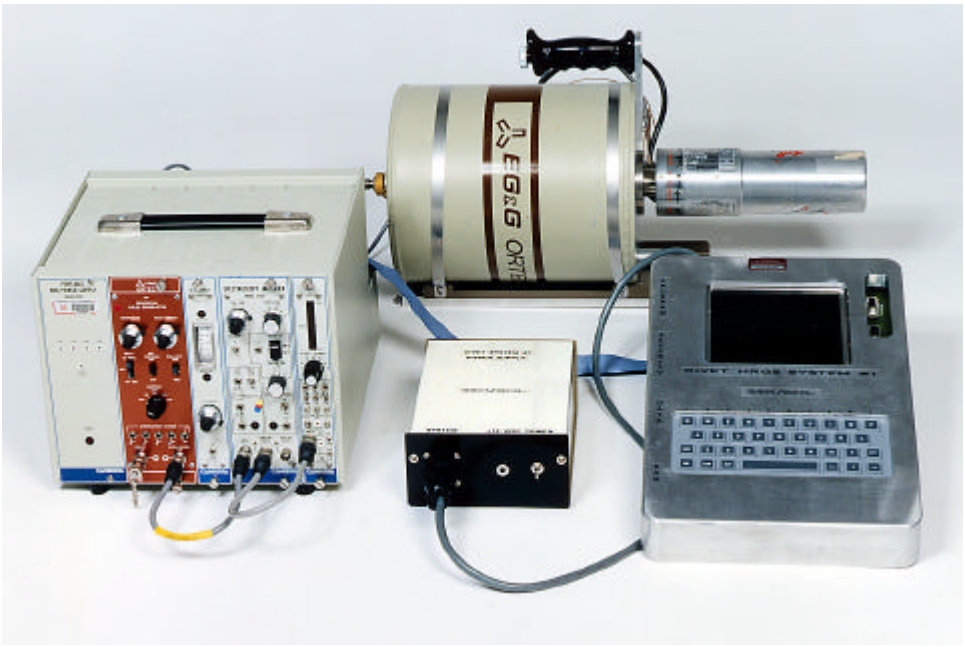

Figure 4. CIVET Information Barrier Hardware System

Conclusion:

The CIVET System provides a complete software and hardware information barrier system that has been tested in field trials on actual treaty limited items. The CIVET system is the only implementation of a fully inspectable hardware and software information barrier system in existence at this time.

REFERENCES:

[1]Sastre, C., Sanborn, J., and Indusi, J., "CIVET – A Controlled Intrusiveness Verification Technology," *Verification Technologies*, March/April 1991.

[2]Waymire, D.R., Marlow, K.W., Mitchell, D.J., Scott, H.L., Murray, W.S., Undem, H.A., and Heasler, P.G., "Maturity and Feasibility Assessment of the BNL CIVET Concept and System," SRC-016/94, November 1994.

[3]Geelhood, B., "Information Barriers to Protect Sensitive Information During Nuclear Weapons and Materials Inspections," PNNL-11982, Limited Distribution, September 2, 1998.