Presented at The Annual Meeting of the Institute of Nuclear Materials Management, Indian Wells, CA, July 2001

Study of the CIVET Design of a Trusted Processor for Non-intrusive Measurements*

Peter E. Vanier, Peter Zuhoski and Cynthia A. Salwen
Brookhaven National Laboratory, Upton, New York

Leon Forman
Ion Focus Technology, Stony Brook, New York

Andrey Sviridov, Nikolai Isaev, Victor Chebykine
All-Russian Research Institute of Automatics

Y. Seldiakov *(Green Star Ltd.)*

Abstract

In the early 1990's, Brookhaven National Laboratory (BNL) developed a prototype computer for non-intrusive measurements of sensitive items. The Controlled Intrusiveness Verification Technology (CIVET) system contained a single digital circuit board, custom-designed to perform limited functions. The design was intended to be capable of processing classified data in a secure manner, while displaying only non-sensitive information to the observer. The CIVET hardware and software were deliberately constructed so as to be easy to authenticate. A team of Russian technical experts led by the All-Russian Research Institute of Automatics (VNIIA) is now studying this technology to determine its potential merits and deficiencies.

Introduction

During the early 1990's, a prototype computerized measurement system was developed at BNL as an example of a device capable of performing confirmatory tests on classified items such as nuclear warheads and components without revealing sensitive information[1]. The CIVET system consisted of a high-purity germanium gamma-ray detector and a data-acquisition system controlled by a single-purpose, custom-built computer system. The embedded-processor hardware and software were deliberately designed with a simple, open architecture so as to facilitate authentication by an independent observer. Since that time, several more modern measurement systems have been developed which incorporate features that have come to be known as "information barriers" designed to protect classified information while providing a useful non-sensitive output. Each system has its own unique features, which may represent advantages or disadvantages in different situations, and which are often viewed differently by different technical experts. The choice of design features which may ultimately be employed in the monitoring of international agreements will depend on the opinions and the needs of all parties to the agreements. This paper describes an ongoing collaboration between BNL and VNIIA in which the hardware design and software code used in the CIVET system are independently evaluated by technical experts at VNIIA and other collaborating institutes.

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

[1] Zuhoski, P.B, Indusi, J.P. and Vanier, P.E., "Building a dedicated information barrier system for warhead and sensitive item verification", *Annual Meeting of the Institute of Nuclear Materials Management*, Phoenix, AZ, July 1999

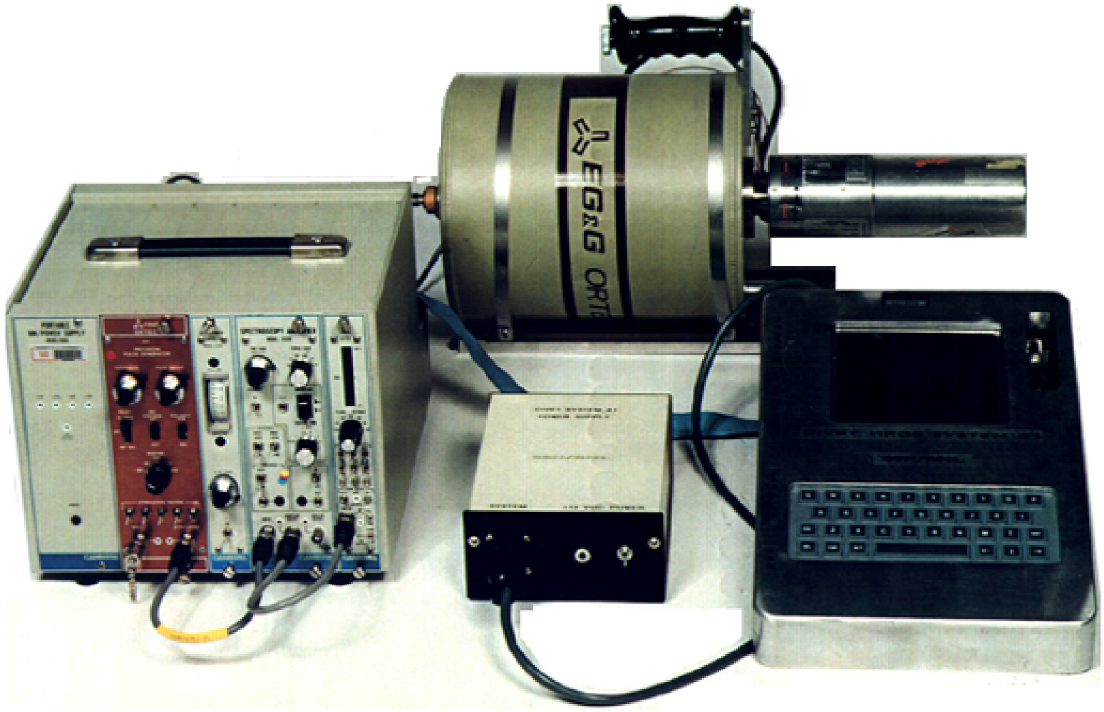

Figure 1. CIVET HRGS system

Overview of CIVET Hardware

The complete CIVET high resolution gamma spectroscopy system is shown in Figure 1. Some components of the hardware, such as the Ge detector, the high voltage power supply, the spectroscopy amplifier and the analog-to-digital converter (ADC) were commercial modules that were considered relatively straightforward to authenticate. The most important part of the CIVET hardware, the digital processor board, which can be considered a prototype "trusted processor", is contained in the custom-built box on the right. The processor board was constructed with considerable attention paid to visibility of the components and their interconnections.

A schematic of the functional areas of the board is shown in Figure 2. The four removable PCMCIA cards shown at the top of the figure are used for storage of all software and data. The executable program for performing all functions is stored in the Program card at the left. The second card is the Security card, provided by the Monitoring party, containing up to 8 bits of error-detection code for every 16-bit word of the agreed executable code. This card also contains encryption data to unscramble the address lines used to access the third card, which will contain Template data to be controlled by the Host. The hardware design and the type of cards ensure that the Program and the Security data cannot be modified while installed in the CIVET system. The fourth card acts as volatile random access memory (RAM) for accumulation of a spectrum and data analysis and any other RAM need by the program. These four PCMCIA cards are the only memory in the system.

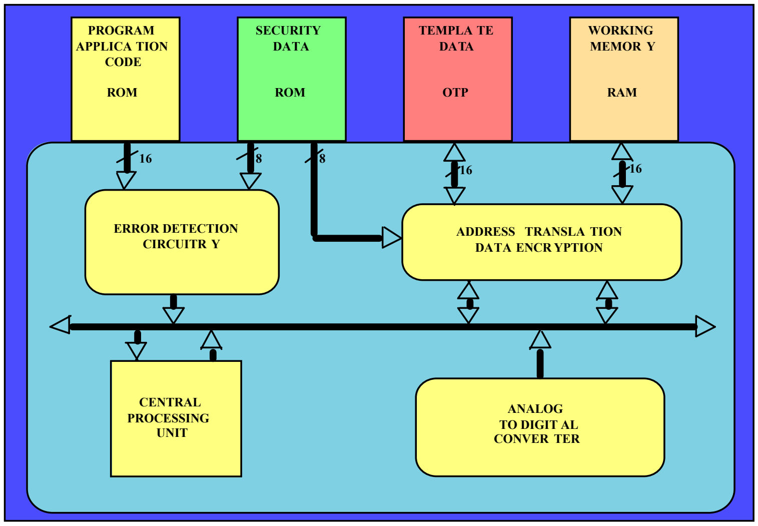

Figure 2. Functional Schematic of CIVET Board

The heart of the processor board is an 80186 EB chip (along with an optional floating point processor chip) whose complete specification, including die metallization patterns, are available for inspection. In addition, there are groups of two other types of chips: Programmable Logic Devices (PLD's), which are preloaded with firmware, and Field Programmable Gate Arrays which are explicitly set up by data in the Program card after boot-up.

Operator inputs to the system are limited to simple keystrokes on a keypad consisting of an array of passive switches which have no interrupt capability. The switch positions must be read by explicit software. The routines to read the keypad are only called when the program is calling for menu-selection input. There are no BIOS (basic input-output system) chips or libraries, which could be difficult to authenticate. Data input from the ADC is via a parallel port, which sends an interrupt signal when a gamma-ray event is detected.

The built-in display device is a liquid crystal array with a simple character-generating controller chip. Some effort would be required to authenticate this and other semiconductor devices in the system by various methods. It would be important to show that they have no extraneous logic functions nor data storage capability. This can be accomplished by random selection from a large number of similar items and destructive testing of a sample selected at the same time as the installed component.

Overview of CIVET Software

All the software was compiled, linked and loaded on a desktop DOS-based computer and then loaded into the Program card using a peripheral PCMCIA drive. The CIVET system itself was not capable of modifying the executable code. In order to verify that the executable code is exactly what was specified by the source code, both host and monitor should separately prepare PCMCIA PROMs using the same version of each compiler, and a byte-by-byte comparison of the executables should be performed. CIVET has no "operating system" and only executes the code agreed upon by the parties.

On boot-up, the microprocessor addresses a fixed starting location in the Program card. Each word of the program is checked by an error-detection algorithm that was previously burned into the set of PLDs. The algorithm checks each program word against a byte of data in the Security card provided by the monitoring party. If there is agreement, the word is loaded into the processor for execution. If an error is detected, the instruction is not loaded into the processor and execution is halted. This feature affords the Monitor the capability to determine that the error-detection algorithm has been correctly burned into the PLD's. The correct firmware ensures that the only code executed comes from the Program card and is consistent with the data on the Security card. The second byte in each word of the security data is reserved for encrypting the data to be stored on the Template card.

The first part of the code, written in assembler, performs some initializations and enables some operations such as the clock and the interrupt-handling routines. A block of binary data is used to set up the Field Programmable Gate Arrays, which are used to interface to the parallel input port (connected to the ADC), the memory cards, the keyboard and the display. A set of replacement library functions obtained from Paradigm Systems Inc., a development tools company, is included to emulate calls to a Disk Operating System (DOS) which might be made by a C program intended to run under DOS. These libraries allow C programs to be developed and compiled on DOS-based desktop computers using compilers intended for use developing DOS programs and then run on the embedded processor, which does not support DOS functions.

The main program, written in C, presents the operator with a menu of necessary functions including calibration of the detector, acquisition of data, and comparison of templates. Some additional routines for analysis of peak areas and computation of statistical parameters were written in Fortran by Ray Gunnink, formerly of Lawrence Livermore National Laboratory.

Russian Evaluation of Strengths and Weaknesses of CIVET Design

Practically from the beginning of negotiations on nuclear arms reduction, work began in both the United States and in the Russian Federation related to the possible future inventory measurements of weapon-grade nuclear material. Information barriers are being studied in both countries in conjunction with radiation measurement systems to potentially help solve transparency issues with nuclear warheads, warhead components, and fissile material associated with warheads. A radiation detection system information barrier (IB) consists of procedures and technology that prevent the release of sensitive information during inspection of a sensitive item, and provides confidence that the measurement system functions exactly as designed and constructed.

One of the first radiation systems for monitoring sensitive items was developed at BNL in 1990. This activity resulted from a BNL proposal to use technology to limit the intrusiveness of a high-resolution radiographic system for containers housing a sensitive item. The project was re-directed from radiography to spectroscopy at an early stage. It was believed by DOE at that time that a gamma-ray spectrometer of limited intrusiveness would be of more generic use to the arms control community, and would, if the problems associated with this development were overcome, clearly demonstrate important technological concepts. BNL was quite successful in completing this effort, calling their system "CIVET" for Controlled Intrusiveness Verification Technology. CIVET embodied such advanced concepts as fully-documented embedded system software, and self-tests for system configuration authentication.

A team of Russian technical experts led by VNIIA is now studying this technology. An analysis of this design is being conducted in order to benefit from the research decisions for development in Russia of similar systems. The potential merits and deficiencies of the CIVET system are considered from a standpoint of non-intrusiveness of the radiation measurements, as well as the potential to authenticate the system and its key components.

The main task of the system is acquisition and processing of sensitive information while ensuring a high level of confidentiality of results of measurements. The concept of the project is to demonstrate 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.

Measurement Intrusiveness Analysis for Gamma Spectrometry of Objects Containing Plutonium

The high level of trust of both interacting sides in the results of plutonium monitoring tests shall be provided by the openness of the measuring system and assurance in the measurement ***non-intrusiveness.*** For this reason it is essential to consider the gamma spectrometer structure and the part of the attribute measurement system related to gamma measurements from the point of view of sensitive information security and prevention of measurement intrusiveness. That is why it would be reasonable to consider this problem both from the position of the sensitive information ***guard*** (with a desire to secure sensitive information) and from the position of a ***violator*** (with a desire to discover sensitive information or falsify measurement results). Figure 3 shows the block-diagram of a system that is used to confirm the presence of plutonium in the controlled object (the first attribute) and the assignment of plutonium in the object to a certain grade (the second attribute). This figure illustrates potential "weak" points in a hypothetical system, the functions of which may not be apparent. Using this illustration, it is possible to examine the intrusiveness of this system and to describe possible measures to increase confidence in the output.

1. Non-intrusiveness of the attribute control system from the GUARD's position.

If the examined system uses the CIVET concept, it shall substantially provide the safety of sensitive information. One typical "weak" place in such a system is the gamma spectrometer itself. Two prototype systems demonstrated by the US DOE laboratories use commercial proprietary multichannel analyzers: the ***Inspector*** (made by Canberra) or the ***DSpec*** (made by ORTEC). These instruments contain many logic and memory components that have to be checked and verified. Also, they are sometimes controlled by a Notebook PC, which also contains such undocumented electronic components. So the openness of both industrial spectrometry systems is not complete. In contrast, the CIVET system acquires a spectrum using only a commercial ADC and a custom-built logic board with limited functionality.

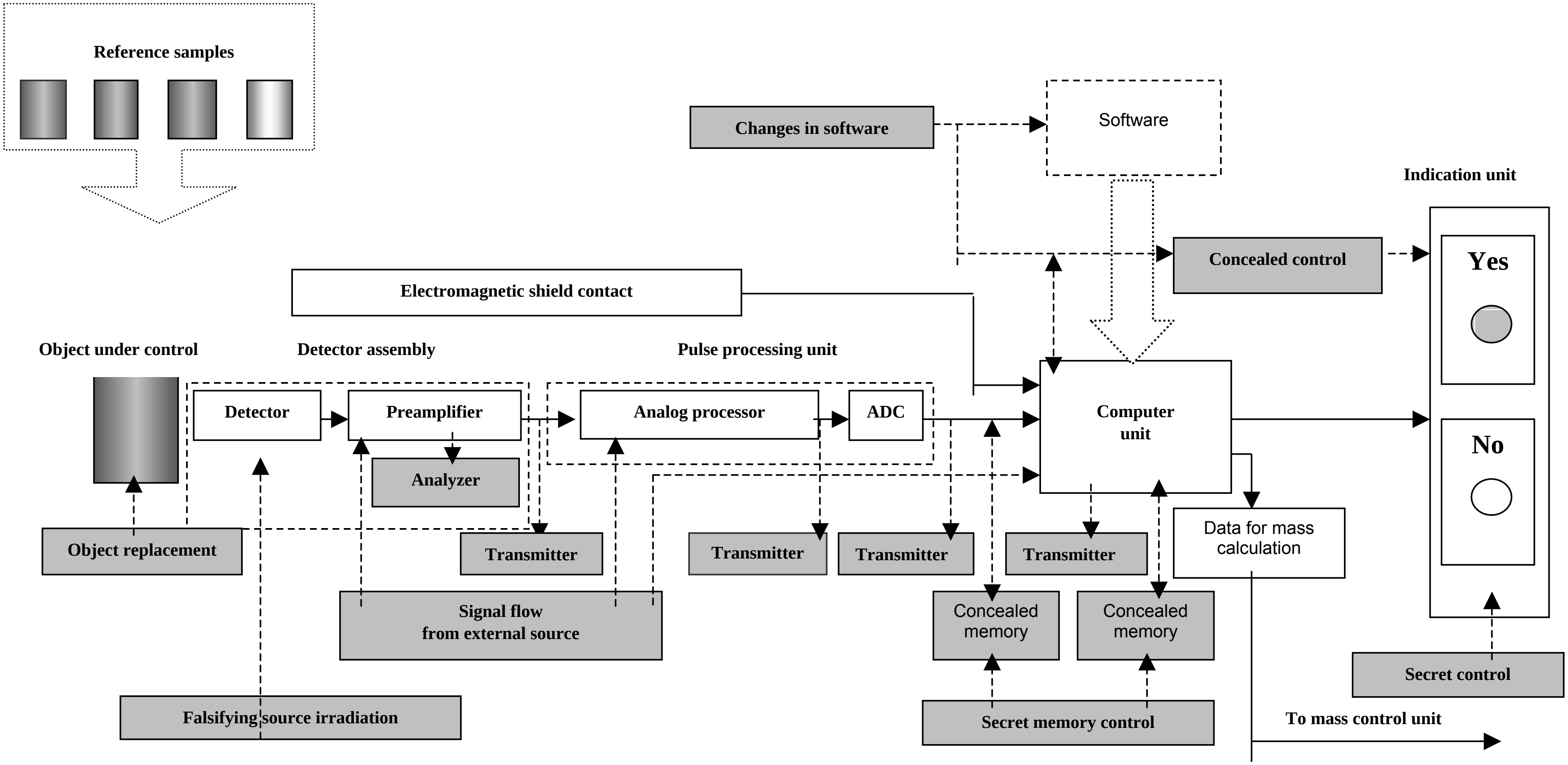

Fig. 3. The block diagram of a system for plutonium attribute control (determination of the presence of plutonium and the plutonium grade in the controlled object). Only one indication unit is shown. Grey colored blocks might be used for measurement intrusion (for explanations see text).

2. Intrusiveness of the attribute control system from the VIOLATOR's position.

First it should be noticed that the violator may use gamma-radiation, electromagnetic pulsed radiation in the visual range (modulated visual or IR), RF range and also audio and ultrasonic signals to distort or transmit/receive information.

Countermeasures

- Representatives of interacting sides (host and monitor) should be dressed in special clothing and before going to the measurement zone they should be checked with a metal detector and a dosimeter by a person who is responsible for on-site security. Private items also should be checked (eyeglasses, rings, writing objects, hearing aid, badges, etc.).
- Measurement zones should be equipped with warning indicators of above mentioned radiation and signals.
- The system and its parts should have only those communication lines and links required by the documentation. This should prevent sending and receiving unforeseen or unauthorized information and signals.
- A single button (key) pressing should start the measurements.

Further measures will be described for preventing access to sensitive information and its disclosure.

Object under control

This is the main source of controlled and sensitive information. The monitoring side has to have full confidence that the object under control generated the measurement information for the system. To falsify the measurement results violator may either replace the object under control by another one or secretly irradiate (through the wall, ceiling or floor) the measurement position.

Countermeasures

- To exclude the replacement of the controlled object, its positioning on the measurement place and the shield closing must be done in the presence of the monitoring side.
- Before and during the measurements the gamma background should be measured to determine and/or avoid the irradiation of the measurement position by a hidden source.
- For this purpose a radiation shield should protect the measurement position.
- During measurements the measurement place must be visually controlled.

Detector assembly

This component generates the primary information in the form of analog signals. The violator might transmit to it a signal pulse train from an external source (through communication links) or secretly pick up the information using appropriate devices.

Countermeasures

- Since the detector assembly is an industrial product it should be checked to determine the absence of any additional circuits (not included in its documentation) that might send or store measurement information or receive external signals. Extremely small pulse analyzers have been developed recently. These instruments might store measurement data, and must be excluded.

- All preamplifier electronic components should be checked to determine that they meet specifications (ADC, memory chips looking like capacitors, resistors, etc.).
- The preamplifier circuits should not contain any power sources (batteries, etc.) that may power extraneous circuits (e.g. transmitters and memory).
- The simplest way to discover a concealed power source is to measure the voltage in the preamplifier circuit when the power is turned off.
- The only communication and power lines that come to the detector assembly should be those required by the documentation.
- During the measurement, no external signals should be fed to the detector assembly.
- The detector assembly power lines should be free of any information signals.

The Pulse Processing Unit.

This is one of the most important parts of the system. This unit processes the signal and digitally codes it. The violator might send to it a sequence of signal pulses from an external source (through a communication line), secretly pickup the information using a transmitter or store the data in a concealed memory.

Countermeasures

- Since the pulse processing unit is an industrial product it should be checked to determine the absence of any additional circuits (not included in its documentation) that may send or store measurement information or receive external signals.
- The unit circuitry should not have nonvolatile data memory.
- To improve the sensitive information security the ADC may operate in certain assigned energy windows. In this case the computing unit shall receive only a part of sensitive information that would be used to calculate the isotope ratio.
- All electronic components of the unit should be checked to determine masked ones (looking like capacitors, resistors, etc.).
- The unit circuits should not contain any power sources (batteries, etc.) that may power extraneous circuits (e.g. converters and memory).
- The simplest way to discover the concealed power source is to measure the voltage in the unit circuits when the power is turned off.
- The only communication and power lines that come to the pulse processing unit should be those required by the documentation.
- During the object measurement no external signals (except the detector assembly ones) should be fed to the unit.
- The power lines to the unit should be free of any information signals.
-

The Computer Unit

The design of the computer unit and its parts have to be "open". The intruder may send to it a false spectrum from an external source (through the communication line or by RF transmission), secretly pickup the information using a transmitting device or save the coded information in a hidden memory.

Countermeasures

- The computer unit should be checked by running a test program that must verify the unit configuration and determine the presence of unintended circuits. This is one of the possible "weak" features of the unit and special attention will be paid on it on the further stages of the work.
- The unit should not have nonvolatile storage devices.
- All electronic components of the unit should be checked to determine disguised devices (looking like capacitors, resistors, etc.).
- The unit circuits should not contain any power sources (batteries, etc.) that may power extraneous circuits (e.g. converters and memory).
- The power lines to the unit should be free of any information signals.
- The simplest way to determine the concealed power source is to measure the voltage in the unit circuits when the power is turned off.
- The only communication and power lines that come to the computer unit should be those required by the documentation.

Software

The software consists of **an executable program** that controls the measurement mode, processes the spectrum, calculates parameters such as the isotope ratio, compares the final data with the threshold values or with a template, allows sending of output indication signals and **supporting programs** that help the execution of the main program and provide additional functions (menu, calibration, input/output control, etc.). The violator might make changes in the software to distort or falsify the measurement results or change the measurement mode settings.

Countermeasure

- A modular principle should be used in the software development to simplify the checking and verification of the programs using checksums and other methods. The block design would allow tracing any changes and insertions in the software (for example, the generation of a false output triggered by a certain hidden input – e.g. a radioactive label in or on the controlled object). Certain measures to provide the software safety and its intrusiveness resistance will be proposed on the further stages of this work.

The Display Unit

This unit is the simplest part of the system but at the same time the most important one since its signals inform the controlling side about the final results of checking an object. The violator may secretly send to this unit the wrong control signals that may falsify the results.

Countermeasures

- The unit should be in conformity with its technical documentation.
- The signals that activate the indicators should be DC logic level ones
- The unit communication lines should be free of any other information signals.
- The only communication lines that come to the display unit should be those required by the documentation.

System Function Verification.

Before the measurements and during them the interacting sides should check the performance functions of the system to assure the measurement results can be trusted. The violator might change the plutonium grade threshold value.

Countermeasures

- To verify the system functioning certified unclassified reference samples with known isotope ratio and mass should be used.
- The physical properties of these samples (composition, mass, dimensions, container thickness and material, etc.) should as much as possible correspond to the objects to be controlled.
- It is most desirable that the set of reference samples should have the isotope ratio above and below the threshold value.

The discussed list of countermeasures is intended to improve the measurement non-intrusiveness. The proposed countermeasures may contribute to other safety measures related to the sensitive information security during international inventory inspections of objects containing plutonium and consequently strengthen the confidence in the inspection results.

Conclusions

- This study has examined 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.
- The principles used in building the CIVET system provide some solutions to the problem of performing non-intrusive measurements and allowing simple authentication of the system. The concepts of the CIVET design establish a framework and a perspective for looking at future systems. In making further improvements to the system and in the development of similar systems it is reasonable to retain some of these concepts.
- Merits of the system: a simple hardware base, presence of rather detailed documentation, verifiable hardware components, restrictions on software to avoid unauthorized functionality, absence of an operating system, verifiability (the test-program) of software and encoding of information.
- Questions for further study: the need to protect system from electromagnetic and ionizing radiation, finding the «bookmarks» (where additional information might be inserted), the use in CIVET software of commercial libraries (Microsoft compilers and the Paradigm Locate embedded system development package), a description of which was not available.
- The analysis of publications on the CIVET system and studies on measures to improve information security of systems for monitoring objects containing plutonium have shown a need for taking additional steps for protection of sensitive information. The most reasonable approach is to use a sequence of information barriers and to take additional measures to authenticate both the construction of the computer unit and the software.
- Realization of these developing technologies will promote increasing of confidence when monitoring objects contain special nuclear material.