
**BNL-90156-1988**

# *CIVET a Controlled Intrusiveness Verification Technology*

**Cesar Sastre**

December 1988

**Nonproliferation and National Security Department**

**Brookhaven National Laboratory**
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

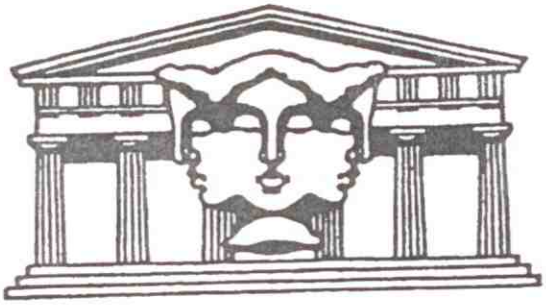
# DISCLAIMER

UNCLASSIFIED [redacted]

[redacted]

[redacted]
CIVET (Controlled Intrusiveness
Verification Technology) [redacted]

# CIVET



a

## Controlled Intrusiveness

## Verification Technology

by


**Cesar Sastre, TSO**

**BROOKHAVEN NATIONAL LABORATORY**


Declassified by:
Peter Vanier, DC,
NNS Department
Declassified by:
Joseph P. Indusi, DD
NNS Department
Derived from:
CG-ACVT-1, September 1,
2005, DOE
Declassified on:
March 14, 2007

**December 1988**

[redacted]
Unauthorized disclosure [redacted] and
administrative sanctions.
Derivative Classifier: [redacted]
Head TSO, BNL
(Title)
OADR
(Date, Event, or OADR)
Derivatively classified by: CG-ACVT-1
(Guide or Source Document)

UNCLASSIFIED

[redacted]

## SUMMARY

CIVET is a proposed concept for Arms Control verification capable of using information while preserving its confidentiality, in a bilateral environment.

## INTRODUCTION

This is a concept definition of a technology for arms control verification, that would permit to automatically limit the disclosed information below a predetermined acceptable level of intrusiveness, without actually limiting the information used in making the verification finding. For the purpose of identification we call this concept Controlled Intrusiveness Verification Technology (CIVET).

CIVET is based on the recognition that there is a substantial difference between the detailed information needed to verify the presence of nuclear warheads in a vehicle and the limited information that the parties to a treaty would be willing to disclose to each other. It is also based on the idea that the technology for doing the measurements needed for verification is largely available, but that unrestricted used of the best measurements techniques may reveal too much of the details of construction of nuclear weapons.

Assume, just for the sake of illustration, the following totally unrealistic scenario. An impartial and knowledgeable inspector is allowed by the inspected party to gain complete access to a vehicle, and is allowed to convey to the other inspectors of the inspecting party his or her finding of whether the vehicle contains contraband or not, using a communication channel that allows only one bit of information across, and assume that the inspector's memory of the occasion is reliably erased afterwards.

In such an implausible arrangement, any information gained by the inspector and used to reach the finding of verification, would be not be available to the inspecting party.

Such system, if it were practicable, should in principle be acceptable to both parties.

To avoid the obvious practical problems with the system just described, CIVET replaces the trusted inspector by an automated measuring system

programmed to reveal only information mutually agreed by the parties and constructed in such a manner that no information is retained after the measurement and no information is transmitted to the inspecting party other than what is mutually agreed to be displayed by the system.

An integral part of the CIVET concept is a series of principles and rules that in concert make the system workable.

The conceptual scheme of CIVET aims to strictly adhere to the rule of symmetry of procedures. That is, that the measurements and techniques used in verification are applied equally to both parties.

During an given inspection, the concerns of both parties are different. If the inspected party cheats and is uncovered several days later, the resulting miscounting of the warheads in a few missiles for a few days is probably not too serious for the inspecting party. On the other hand, if the inspecting party uncovers a piece of weapons design information that is classified, that particular loss for the inspected party is irreversible, and essentially instantaneous. This asymmetry is used in CIVET to select the parties having control of the equipment immediately prior to the inspection, and following the inspection.

CIVET requires **no encryption** to protect the integrity of the data, or secrecy of design for its operation.

## FUNCTIONAL STRUCTURE - HARDWARE

A verification system could be viewed as composed of three parts, a sensor subsystem, a data processing and control hardware subsystem, and a data processing and control software subsystem. This later subsystem is described in the next section.

### Sensors

The sensor subsystem is determined by the measurement or set of measurements that are necessary for the verification of the statement in question. A statement in this context is understood as a clearly formulated, unambiguous sentence such as *"there are no more than 7 nuclear warheads in this can"*. The choice of sensors is not limited by considerations of protection of sensitive information since this function is built into the design and the procedural rules.

The only limitation on choice of the detectors is in the technology embodied in the sensors themselves, which the parties might not want to share.

In principle detectors other than nuclear radiation sensitive, or nuclear particle sensitive, could be used singly or in combination with nuclear radiation sensitive devices to produce an unambiguous signature.

**Radiation detectors**

Radiation detectors could be X-Ray and/or gamma sensitive, and be configured as open, collimated, or in arrays (as would be used in a hodoscope system). It is assumed that the choice of detectors would be dictated by adequacy for the mission, lowest technology compatible with the mission, and economy.

**Interrogation system**

For the verification of cases where the objects are such that self-shielding introduces uncertainties in the verification, the designer would be free to consider X-Ray, gamma or neutron sources to excite the target to produce a useful signature.

**Positioning Devices**

For many of the measurement schemes, the positioning of detectors and sources could be controlled by use of simple fixtures. However, we should not rule out the use of robotic arms to move the interrogation source and the detector about the object to be verified, to search for warhead patterns. If the position of the source or the detector needs to be changed to accomplish the measurement, it is assumed that it would be done either directly under the control of the computer, or indirectly by humans following directives flashed on a video display terminal by the computer. It is important that inspectors are not allowed any arbitrary decision–making in the positioning of detectors or sources. It is also assumed that the design of the logic of the positioning controller be such that the pattern of search produced by the machine gives no clues about the weapon design.

**Signal Conditioners**

The output of radiation detectors will in general require amplification, discrimination, pulse shaping, isolation, and impedance matching. To the largest

extent possible any adjustment or calibration of the parameters of the signal conditioners should be under the direct control of the computer, and should produce no external display of the pulse arrival time or count rate, or emanations that could reveal the same.

**Power Supplies**

Low voltage and high voltage supplies that may be needed for detectors, active interrogation devices, and signal conditioners, are adjusted either through hard-wired settings, or are under computer control. That is, no knobs in the front panel, only soldered jumpers inside the chassis.

**Data processing and control**

All functions of control of the sensors and data conditioner, as well as all data reduction and interpretation will be performed by the computer.

**Computer**

The computer should be a readily available low-tech machine such as a modified AT clone, for which replacement boards are readily available. The machine should have no components that would be able to store information in non-volatile memory. No hard disk, no CMOS memories, and perhaps not even batteries for clocks. All operations should be conducted in volatile memory. This will probably require extra RAM for a ramdisk. All software will be loaded just prior to the verification measurements through floppy drives hardwired for read–only operation.

**Data Interface**

The computer shall be provided with a general purpose interface bus, so that different sensor systems and positioning devices may be accommodated. The object is to make the computer as standard throughout the arms control verification effort as possible.

## FUNCTIONAL STRUCTURE - SOFTWARE

The principal design criterion for the software is that it should be robust enough to perform the measurements, and make the determination required for

verification over the range of situations that it may encounter in the field, without asking for instructions or revealing by its behavior what the sensors see. This means that the screen display should be as uninformative as possible.

**Controller - Timer**

The measurement cycle should be of a fixed duration, to avoid signaling to an observer anything about the raw data being received.

**Data Reduction Algorithms**

It is expected that the data to be processed will consist in most cases of count rate vs. position. The algorithms used in the analysis should be, to the extent possible, insensitive to the absolute value of the position. That is, they should be of the pattern recognition type.

**Expert System**

Since the system is supposed to operate in unattended mode, without asking an operator for advice on problems that may arise, a small knowledge based system may be included, to handle optional strategies for the measurement. For example, if the count rates are below some threshold, the expert system could call for a confirmatory new measurement.

## PROCEDURAL STRUCTURE

The functioning of CIVET is extremely dependent on the adequacy of the procedures associated with it.

**Systems Development**

The hardware should be, either developed in cooperation between the two parties, or developed by one and complete details given to the other. In particular the software used should be developed and negotiated between both parties, and tested also by both parties.

**Operations**

We assume that a CIVET system is used for **equivalent** verification scenarios in both countries, using identical hardware and software, and that both countries have copies of the system. For the sake of this discussion we assume that Country A is being inspected by Country B. The sequence of operations is shown in the following page.

Country A has had the complete CIVET package under his control for some time, and has thoroughly, checked it in his laboratory for functionality, and to verify that there are no clandestine devices that could covertly transmit information about the raw data from the sensors to the inspecting party. In other words, Country A knows that before the inspection the CIVET package is clean. Country B inspectors do not participate in this phase of the work.

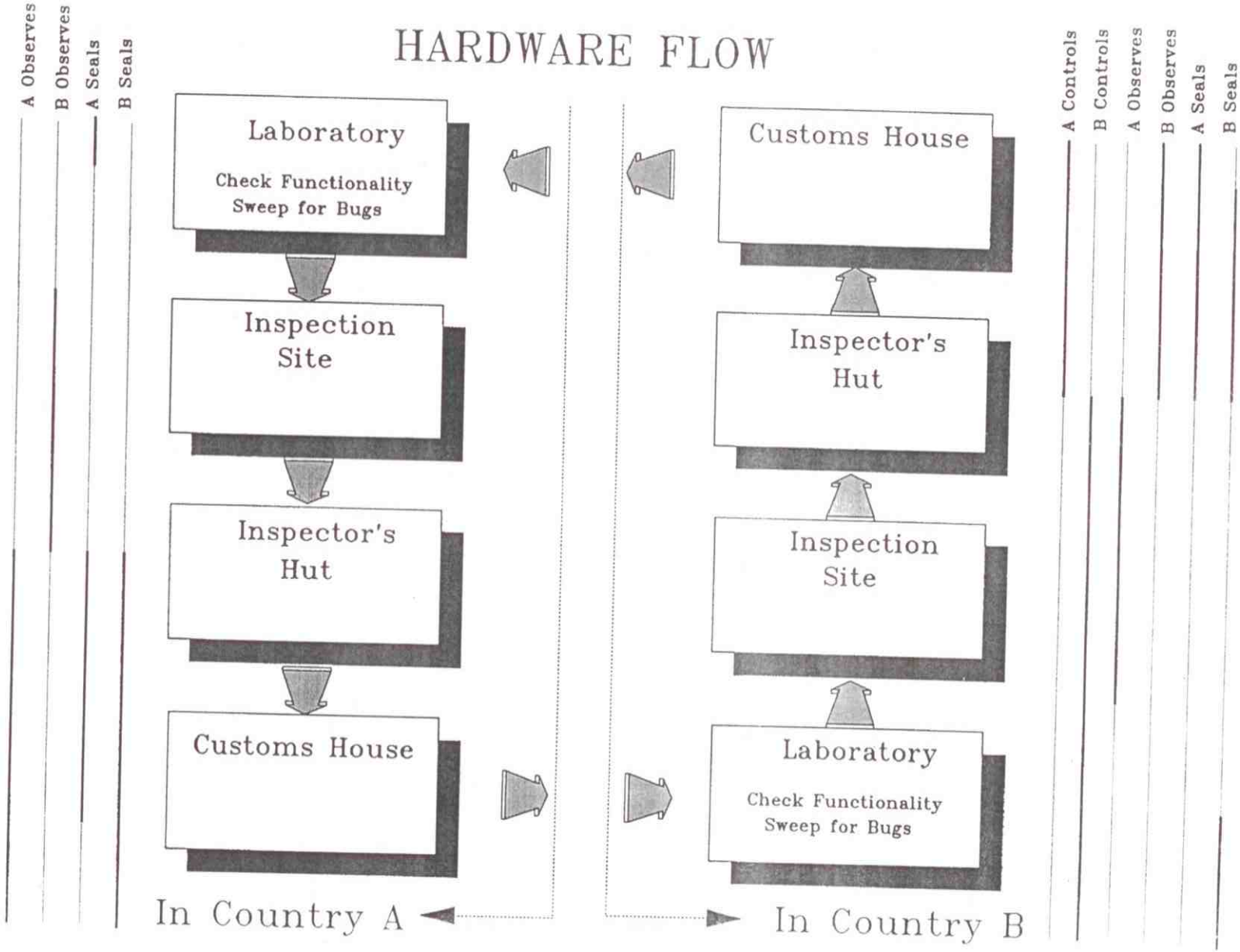
The CIVET package is transported to the inspection site, and prior to the measurements Country B start surveiling the package which is still under the control of Country A.

Country A personnel positions the sensor system about the vehicle to be verified, under Country B inspector surveillance. Country A loads the software into the computer and gives the diskettes, containing the copy of the software, to the Country B inspectors to keep, and take home, where they can verify that the program is clean. The inspectors from Country B could optionally verify the disks in place if they had a computer available.

After the verification measurement is completed, and the results recorded by both the Country A, and Country B personnel, the CIVET package is moved to the Country B inspector's office under constant surveillance by inspectors from both countries. The CIVET package is placed in a shipping container under surveillance of Country A, and country B inspectors, to make sure that Country A inspectors do not remove tampering evidence, and that country B inspectors do not place contraband in the container. The shipping container is sealed with country A and with Country B seals. At this time Country B takes control of the equipment. If the seals are really excellent, Country A could keep control of the package while shipped within Country A territory. However, at this point in the cycle Country B is the one at highest risk and should have higher priority for control of the CIVET equipment.

The CIVET package is shipped to the customs control point at the border, under Country B control, and Country A and B seals.

# HARDWARE FLOW



Country A verifies through the seal that the shipping container holds only the CIVET equipment, and removes their seal prior to shipment to Country B in a Country B conveyance.

At the arrival at Country B's laboratory, the seal is inspected to verify that there has been no tampering with the CIVET equipment in transit. Country B verifies that there was no tampering to make the equipment produce a false favorable verification, and that the equipment is functional.

The software diskettes are compared with the archival samples to verify that they contain the legitimate program.

At this time Country B can accept the results of the verification measurement.

At the laboratory, Country B checks that no bugs have been placed by country A in the equipment, certifies that the equipment is good and clean, and prepares the equipment to be available for use in turn in Country B when Country A inspectors come.

This closes one half of the cycle of the CIVET equipment. The other half of the cycle, when the equipment is used in Country B, is completely symmetrical.

The host country knows that the equipment used in the measurement could not broadcast raw data to the inspectors because equipment had been taken apart, tested, and put together again by the host country technicians prior to the measurement.

The visiting country knows that the system has not been tampered with to make it fail to detect the presence of nuclear weapons because after the measurement they can take it apart and test it.

Tampering with the equipment would have a high risk of detection because of the schedule of surveillance and the schedule of laboratory testing of the equipment. The visiting team would have to tamper just prior to the measurement, while the equipment is under host country control. The host country team would have to remove the evidence of tampering after the measurement, while the equipment is under visiting country surveillance. The closed design of the hardware, should make that tampering very difficult.

Both countries know that the software is legitimate because they can compare it bit by bit with their our certified copies, and from their own inspection of the hardware they know that the hardware itself can not override the software because there are no ROMs in the system.

Both countries know that tampering with settings by either country at the time of the measurement could be detected because settings are hardwired, inside the chassis, and the equipment is under constant surveillance by both countries through the measurement period.

## DEVELOPMENT STRATEGY

For the development and demonstration of the concept, one should select a simple but meaningful verification scenario. For example, an X-ray imaging measurement, or a perhaps a collimated gamma detector imaging accompanied with an absorption measurement could be selected. At this time, it would appear as if most practical scenarios that could be used for development and demonstration of CIVET are not constrained by existing radiation measurement technology. This is not to say that all sensors are off-the-shelf, but it is expected that any required work on the sensors would be mainly a matter of packaging.

After the scenario has been identified for development, it is necessary to formalize the decision rules, and experimental parameters. In other words, the objective operational definition of a nuclear warhead to be used by the computer in the context of the adopted measuring techniques. This will include things such as, solid angle resolution, energy thresholds, minimum count rates, pattern recognition rules, rules to handle inconclusive results, rules to decide when additional measurements are needed. This area is the most delicate and will require the most thought. CIVET only helps by removing the issue of intelligence gathering from the issue of verification. The issue of when the result of measurement indicate the presence of a nuclear warhead or not, is still there, and needs to be made explicit in computer language.

The computer software could present some practical problems arising mainly from the need for complete disclosure. We might need an operating system, a high level language and a RAM disk program in the public domain. On the other hand we might be able to just purchase well established versions of commercial software that has been available for some time, and convince ourselves that there are no hidden features that would give any party an advantage to cheat.

The computer itself should not present serious difficulties. A nearly obsolete machine such as an AT clone made in third world countries probably has no proprietary information left in it. One should consider the possibility of purchasing initially a large number of motherboards and cards of identical design to insure continuity and ease of replacement and verification. Extensive procedures for testing of the hardware will have to be developed for use by the verification laboratories to certify that the machines are clean.