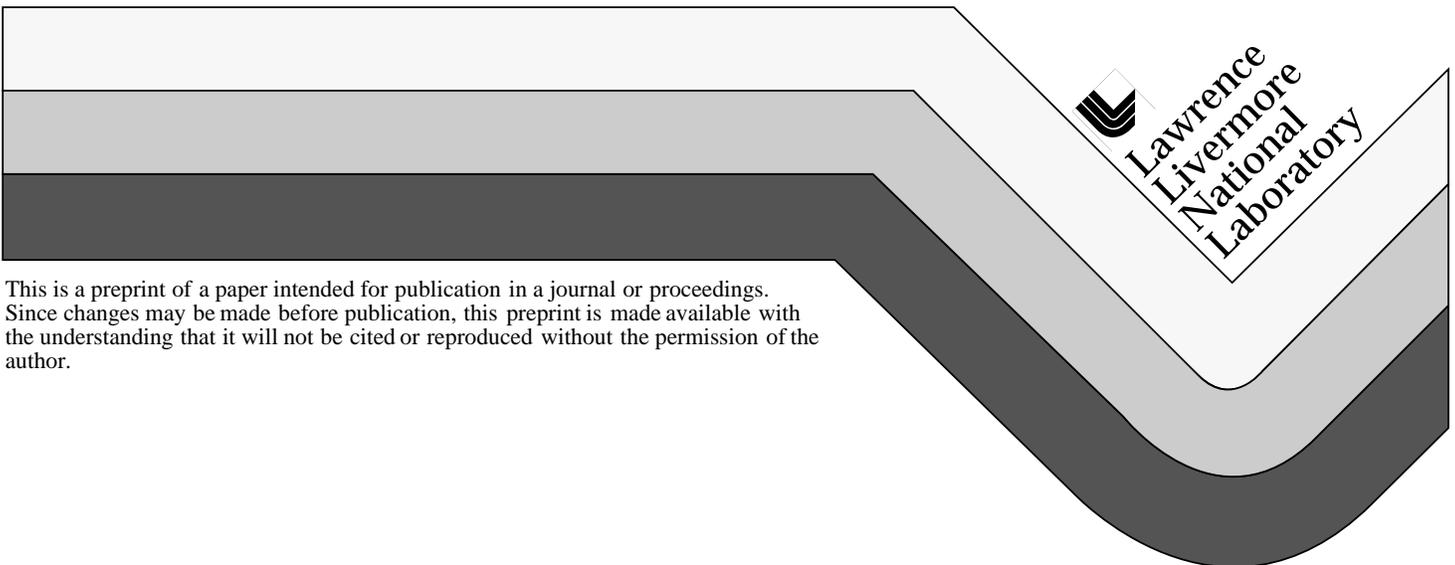


# Safeguards for Nuclear Material Transparency Monitoring

J.K. Wolford  
D.A. MacArthur

This paper was prepared for submittal to the  
*Society of Photo-Optical Instrumentation Engineers*  
*Penetrating Radiation Systems and Applications Conference*  
*Denver, CO*  
*July 18-23, 1999*

June 2, 1999



This is a preprint of a paper intended for publication in a journal or proceedings.  
Since changes may be made before publication, this preprint is made available with  
the understanding that it will not be cited or reproduced without the permission of the  
author.

#### DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

# Safeguards for Nuclear Material Transparency Monitoring

James K. Wolford, Jr.<sup>†</sup>

Lawrence Livermore National Laboratory, MS L-183, Livermore, CA 94551

Duncan W. MacArthur<sup>‡</sup>

Los Alamos National Laboratory, MS J-561, Los Alamos, NM 87545

## ABSTRACT

The US and the Russian Federation are currently engaged in negotiating or implementing several nuclear arms and nuclear material control agreements. These involve placing nuclear material in specially designed containers within controlled facilities. Some of the agreements require the removal of nuclear components from stockpile weapons. These components are placed in steel containers that are then sealed and tagged. Current strategies for monitoring the agreements involve taking neutron and gamma radiation measurements of components in their containers to monitor the presence, mass, and composition of plutonium or highly enriched uranium, as well as other attributes that indicate the use of the material in a weapon. If accurate enough to be useful, these measurements will yield data containing information about the design of the weapon being monitored. In each case, the design data are considered sensitive by one or both parties to the agreement. To prevent the disclosure of this information in a bilateral or trilateral inspection scenario, so-called information barriers have evolved. These barriers combine hardware, software, and procedural safeguards to contain the sensitive data within a protected volume, presenting to the inspector only the processed results needed for verification. Interlocks and volatile memory guard against disclosure in case of failure. Implementing these safeguards requires innovation in radiation measurement instruments and data security. Demonstrating their reliability requires independent testing to uncover any flaws in design. This study discusses the general problem and gives a proposed solution for a high resolution gamma ray detection system. It uses historical examples to illustrate the evolution of other successful systems.

**Keywords:** Safeguards, Radiation Detection, Data Security, Arms Control

## 1. INTRODUCTION

Information barriers are a supporting technology for arms control and nuclear material transparency inspections. Such inspections form part of the basis of any agreement, and information barriers can in many cases reduce concern over the unwanted disclosure of information. Simply stated, an information barrier is a combination of hardware, computer software, and human procedures that:

1. Prevents the unintended release of sensitive information during an inspection.
2. Displays a simple but reliable and useful result to the inspector.
3. Includes some check on the integrity of the internal operations which were concealed from the inspector.

The need for information barriers is not unique to the inspections described in this paper. Indeed the concern over revealing too much information exists wherever intrusive inspection techniques are used on items or in facilities considered sensitive. For example, consider inspections of a ship's propeller for the purpose of establishing an upper limit on its thickness. If the shape and composition of the propeller were considered sensitive, an ultrasonic transducer used to gauge the part's thickness would be considered intrusive, since a trained analyst with the complete time domain record of a pulse measurement could derive the sensitive properties. One solution in this case would insert a hidden layer of analysis that would intercept the measured data and extract only the sought-after property, i.e. the thickness of the part. It would then present this result to the inspector in the simplest possible format.

Applying an information barrier to an inspection process forces designers to confront a dilemma; in hiding all but the essential indications from an inspector, one also hides data that would give some assurance that the internal operations proceeded as intended and that the measurement is therefore valid. As the sections below will demonstrate, thoughtful

---

<sup>†</sup> email: [wolford@llnl.gov](mailto:wolford@llnl.gov); telephone: (925) 422-7236; fax: (925) 422-9343

<sup>‡</sup> email: [dmacarthur@lanl.gov](mailto:dmacarthur@lanl.gov); telephone: (505) 667-8943; fax: (505) 665-9277

designs can help recover some of this lost assurance through features that simulate the actions and decisions of a human operator.

## 2. HISTORICAL PERSPECTIVE

The notion of an information barrier has actually been around for decades, though the nomenclature is more recent. Wherever adversaries have negotiated agreements, and inspections have been instituted to verify those agreements, special care has been taken to ensure that those inspections don't disclose more information than is necessary. Recent examples include the Threshold Test Ban Treaty (TTBT) and the Chemical Weapons Convention (CWC). In the TTBT, a joint verification experiment (JVE) was staged [1988], wherein Soviet representatives were invited to witness an underground test at the Nevada Test Site, and US representatives witnessed a similar demonstration at Semipalatinsk in the Soviet Union. Both sides used a monitoring method known in the US as CORRTEX. In CORRTEX, a time domain signal is generated on a long transmission line, adjacent to the explosion. As the explosion proceeds, the transmission line is shunted by the pressure of the propagating shock. From the velocity of the shock propagation, one can infer the energy yield of the device. Planners on both sides agreed that information from the incipient phase of the explosion was sensitive and agreed mutually to exclude or blank out the first 15 microseconds of the time record. This measure was referred to as an *anti-intrusiveness device* (AID) and, despite its simplicity, was crucial to making the JVE a success. Later, in 1995, negotiations for a more ambitious effort known as the agreement for Mutual Reciprocal Inspections (MRI) broke down. MRI stemmed from a March 1994 agreement between then Energy Secretary O'Leary and Russian Atomic Energy Minister Mikhailov for extensive inspections of plutonium removed from dismantled weapons. Originally the US negotiators had sought and won an amendment to the Atomic Energy Act of 1954 granting limited permission to share certain classes of information with their Russian counterparts. This so-called "agreement for cooperation" was never exercised. Planners had failed to gauge adequately the difficulties the Russian Federation negotiators would encounter in seeking exceptions to their internal state secrets act. Efforts to salvage the agreement then focussed on identifying ways to modify the measurement instruments themselves, to prevent them from displaying to the inspector any data not needed for the verification. These early efforts, while insufficient to revive the MRI negotiations, nevertheless form part of the present-day "defense-in-depth" approach to information barriers.

The Chemical Weapons Convention of 1997 includes provisions for site inspections that aim to verify the absence of certain compounds at industrial and storage facilities. The treaty and its verification annex both stipulate limits on the intrusiveness of measurements. The design of the measurement equipment, including a specially built gas chromatography / mass spectrometry system, includes features to conceal all information not required for the inspection. Specifically, it reports only the presence or absence of those chemical compounds controlled by the agreement.<sup>1</sup>

The lessons of these successes and failures prompted continued development of measurement techniques which contained or lent themselves to the addition of an information barrier. In recent years, solutions to various facets of the problem have evolved at the US Department of Energy (DOE) national labs. For example, the Radiation Inspection System (RIS) developed by Sandia National Laboratories uses the gamma ray spectrum from a sodium iodide detector to distinguish weapons-grade from reactor-grade plutonium.<sup>2</sup> The low resolution of the sodium iodide spectrum precludes a determination of the precise isotopics of the material—information that the Russian Federation considers sensitive and not to be revealed. RIS derives its result from comparing the inspection measurement with a known template. A database of templates is prepared in advance, spanning the complete set of expected sources. One clear advantage of the RIS sodium iodide measurement is its speed; using a 3 cm x 3 cm detector, one can gather enough counts from a typical sample in 30 seconds for an accurate determination. A corresponding measurement from a high purity germanium detector could take typically 900 seconds. Also, sodium iodide detectors operate efficiently at room temperature, avoiding the need for a supply of liquid nitrogen and the inconvenience of maintaining a chilled detector in a field location. The template approach excludes from the inspection process any specific physical attribute, relying instead on the hidden process of template comparison for a judgement of pass or fail. This simplifies the output and eliminates the need for negotiation over attribute threshold values. However, it raises related concerns over the ownership and handling of the template between measurements.

Highly enriched uranium presents special challenges, since, unlike plutonium, it does not produce radiation with energies and intensities sufficient to penetrate optically thick absorbers. Thus passive radiation measurements on assembled weapons containing uranium are difficult. Oak Ridge National Laboratory takes a different approach with its Nuclear Material Identification System (NMIS).<sup>3</sup> NMIS uses active interrogation, allowing the neutrons from a <sup>252</sup>Cf source to induce fission neutrons in the uranium, and monitoring the emissions in a coincidence measurement. The resulting signature is very sensitive to the amount of material in the source and is distinctive enough to differentiate weapon parts from mockups.

In Brookhaven National Laboratory's CIVET (Controlled Intrusiveness Verification Technology) system, engineers concentrated on the control and acquisition hardware with the goal of making it simple to authenticate. It treats as paramount the desire to disclose exhaustively all hardware and software elements of a system, presumably making it easier for technical specialists to understand and trust its operation. They designed enough capability into the main processor to minimize the user's interaction and to preclude the need for display of intermediate results.<sup>4</sup> Its Intel 80186 processor is primitive by contemporary standards, but fully adequate for its calculations. Furthermore it has a simple design, which lends itself well to inspection by x-ray and other standard techniques.

What all of these approaches share in common is their specificity. They address information protection of a specific measurement instrument, or they stress one particular requirement of information barriers in the abstract. So far what's been lacking is a modular solution to the problem of data protection in an inspection regime, one that doesn't rely on a full integration of the measurement instrument and the information barrier and that doesn't depend much, if at all, on the type of measurement device(s) being used. The system presented below takes the first steps toward such a goal.

### 3. CURRENT AND PLANNED MATERIALS AGREEMENTS

The US and the Russian Federation are at various stages of negotiating or preparing to negotiate several arms control and nuclear material transparency agreements. The most visible of these is START III, which will continue the trend in nuclear arms reductions begun with START and START II. Some lesser-known agreements, however, have progressed further in negotiating measurement regimes and are now framing the debate on information protection. These include the Mayak Fissile Material Storage Facility agreement. Under this agreement, the US will supply goods and services to build a new storage facility in Russia near the fuel processing site at Chelyabinsk-65. In return, the Russian Federation will place its material into a transparency regime supervised by the US. One derivative of the Mayak agreement is called the Processing and Packaging Implementation Agreement (PPIA), which concerns monitoring of the facility that will reshape the plutonium prior to storage at Mayak. To address the issue of continued plutonium production in Soviet-era reactors, which are also necessary for power generation, the two sides have negotiated the Plutonium Production Reactor Agreement (PPRA). Methods for inspections under the PPRA are now under discussion. But of all the agreements, the one closest to consensus on measurement technologies and means to protect information is the Trilateral Initiative. Work at Los Alamos National Laboratory (LANL) and Lawrence Livermore National Laboratory (LLNL) on preparing a prototype inspection system for Trilateral Initiative generated most of the ideas presented below.

In September 1996, the Trilateral Initiative was launched by the US Department of Energy (DOE), the Russian Ministry of Atomic Energy (MINATOM), and the International Atomic Energy Agency (IAEA.) Its objective was to provide the technical basis to fulfill an agreement made by Presidents Clinton and Yeltsin to put a large quantity of excess weapon-origin fissile material into storage under international monitoring. The IAEA accepted the task of verifying and providing international confidence that these materials have been irreversibly removed from nuclear weapons programs. DOE's aim was to develop attributes based verification approaches and technologies it could apply to US and Russian storage facilities. First this required that the US and the Russian Federation agree on the relevant physical attributes to be measured during inspections. The information contained in these attributes had to provide confidence that the stored materials being inspected were consistent with the host country declarations. The initial focus was on plutonium, much of it in classified form. All three parties to the agreement assume that the means to perform the more difficult verifications on highly enriched uranium (HEU) will evolve to meet the schedule. The negotiators settled on three plutonium attributes which would provide sufficient confidence: (1) Presence of plutonium in the storage container; (2) an indication of its isotopic composition, specifically, the result of a comparison of the measured ratio of  $^{240}\text{Pu}$  to  $^{239}\text{Pu}$  with a prescribed threshold; and (3) an indication of whether the total mass of plutonium in the sample surpasses another prescribed threshold. Once these physical attributes were established, the measurement techniques were chosen. For the plutonium presence, and ratio determinations, a high purity germanium (HPGe) spectrometer and pulse height analyzer was chosen as a measurement technique. The mass attribute derives from a detailed neutron assay of the amount of  $^{240}\text{Pu}$  present and a knowledge of the isotopic composition.

The same sensitive data concerns that existed for MRI persist for the Trilateral Initiative. Fortunately, the understanding of the technical challenges is more mature on all parts. Perhaps as a consequence, the planners on all sides proposed the use of information barriers from the outset and won agreement for their use at a sufficiently high governmental level. MacArthur and Whiteson have documented requirements which have been provisionally agreed to by the three sides.<sup>5</sup> Preliminary design collaborations led to the creation of a prototype that is currently under review, both inside the US government and by the Russian Federation and IAEA as well.

#### 4. GENERIC DESIGN ELEMENTS

While an actual information barrier will be adapted to the measurement instrument it must accompany, some considerations of information protection require no knowledge of the type of measurement being performed. An information barrier design will always contain the following three elements:

- (1) A means to conceal the primitive information gathered in a measurement, and from which the physical attributes of an inspected item are derived. In some cases, the value of the derived attribute will be sensitive and must be concealed as well. This may be accomplished through hardware, software, human procedures, or a combination. The barrier should work in both directions. It should eliminate or strongly attenuate unintended signals originating on the outside as well as on the inside of a measurement system.
- (2) A simplified display that indicates clearly the selected results of the measurement test as defined in the agreement, and nothing more. In general, the display should be no more complex than is necessary to convey the result to the inspector.
- (3) Enough automation to compensate for the lack of a human operator, both in monitoring the measurement and in safeguarding the data. The instrument must check the reliability of its own measurements as well as protect the data resident during an inspection. In the event of failure or signs of tampering, this mechanism should erase all traces of sensitive data from the instrument and bring the inspection to a halt.

The first element encompasses any form of information transfer indicated in the setting. For example, if the unmodified instrument has a display that gives exhaustive information about the progress of a measurement (which many quality instruments do) then element 1 dictates that the display be disconnected, disabled, or covered up. If the inspector has close access to the instrument, one may additionally need to prevent it from transmitting or receiving signals of a mechanical (seismic, acoustic) or electromagnetic (RF, IR, or undeclared radioactive) origin. Some of these measures are straightforward to instantiate in the design of the instrument, while others must be trusted to written authentication and inspection procedures. (One could conceive of a barrier composed entirely of written procedures, enforced by representatives from each country or organization participating in the agreement. Success in such an arrangement would depend on uncharacteristically flawless human action, and would be labor intensive.) A more likely combination would include a physical shielding barrier to prevent emanations, and a data barrier to control the instrument output and provide an interface to the display.

In the case of a computer-controlled gamma ray spectrometer, the sharp switching waveforms generated by the digital electronics could disclose the internal logic state of the instrument via radiofrequency (RF) emanations. To mitigate this effect, one can enclose the system in a shielded enclosure. Whiteson et al have proposed such a measure for the Trilateral Initiative<sup>6</sup>. A few millimeters of an appropriate conductor, such as steel or copper, properly grounded, would provide an excellent RF shield while remaining essentially transparent to the gamma rays in the range of interest. Commercial shielded enclosures meeting industry and FCC standards are readily available. The enclosure brings the added advantage of preventing any access to or tampering with the detector and its analyzing electronics during a measurement.

The second element replaces the usual instrument interface with a simple set of indicators. There are two design approaches depending on the status of the analyzed information. If the attribute being displayed is not considered sensitive by the inspected party, then the attribute value itself may be displayed, and a numerical readout is appropriate. If instead, the inspected host does not wish the attribute value to be disclosed, then the instrument's processor compares it to a negotiated threshold and displays a binary indication of the result, i.e. a pass or a fail for the comparison test. The parties to the agreement should set the threshold at a value well outside the range likely to be encountered during measurements, so that normal statistical variations do not generate a pattern of passes and fails that would effectively disclose the physical value. The exact implementation of the results display is somewhat arbitrary, though it should lend itself to authentication tests meant to verify that no incidental information is inadvertently or purposefully displayed. Useful examples might include a bank of indicator lights or, for permanent records, a printed hardcopy containing the same simple results.

The third element couples to and enhances the first. For example, to ensure the integrity of a physical barrier, such as the shielded enclosure described above, one can fit the access door with an interlock, designed to withdraw power from the instrument and display whenever the enclosure is opened. By augmenting the interlock with digital circuitry, one can add to the conditions that trigger the shutdown. Using the same example of a physical barrier, likely candidates would include ground faults and software process timeouts (indicating abnormal operations or "hung" processes.) Extending this idea, one could generalize the interlock approach and create a "security watchdog", which not only triggers a shutdown for a list of

error conditions, but could also give a positive indication of status when it judges the system is functioning as intended. The effect of the watchdog is to enforce a set of assertions that should obtain during normal operations, e.g., "the enclosure is sealed", "the enclosure is grounded", and "the processor received the neutron result in less than 10 minutes". The watchdog compensates, in part, for the lack of a human operator and stands by to "pull the plug" in case of malfunction.

Figure 1 shows a high level block diagram illustrating the relationship between the 3 design elements. The acquisition system operates within a barrier, confining the sensitive data to a volume inaccessible to and obscured from the view of the inspector. The results appear on a display which reveals only the required attributes. The security watchdog monitors the status of factors affecting data protection, and terminates the inspection, deleting all gathered data if it detects a security threat.

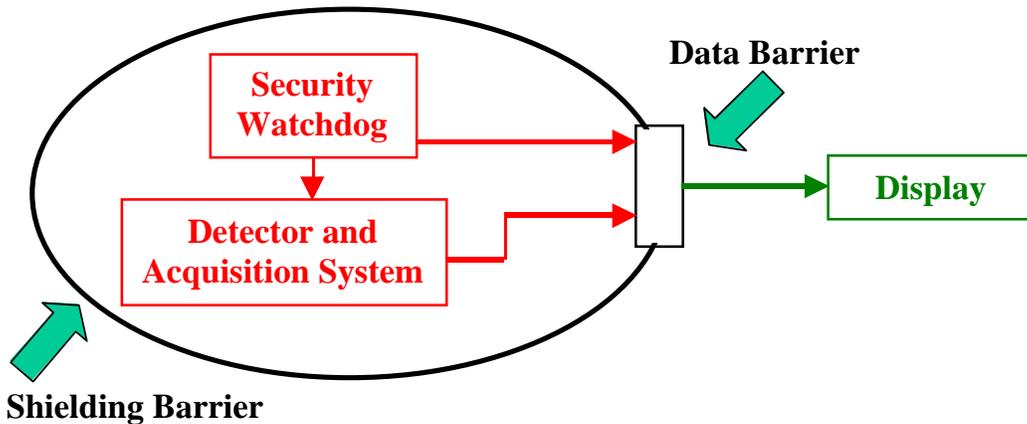


Figure 1. High level block diagram showing the interrelationship between the three design elements. The makeup of the physical barrier enclosing the sensitive data volume depends on the nature of the vulnerabilities. Once the system derives its attribute results, they must pass through an isolation step before crossing the shielding barrier. The data barrier provides this isolation, and also serves as an interface to the display. It ensures that information flows outward only, and that the information contains only the agreed-to indications. The exact format of the display can be shaped by the needs of the inspecting organizations. The security watchdog oversees the acquisition and analysis processes and shuts them down in case the barrier is breached.

In the next section, these design elements are exemplified in a hypothetical gamma ray spectroscopy instrument, which is similar in design to a portion of the Trilateral Initiative prototype system. The specific design of the Trilateral system depends strongly, as does any system, on the circumstances of the agreement. These include the inspection attributes as well as arrangements for the custody of the hardware. In the Trilateral Initiative, the existence of a third organization led to unique requirements, resulting in a unique design.

## 5. EXAMPLE: INFORMATION BARRIER FOR GAMMA RAY MEASUREMENTS

One common, though intrusive, method of identifying the nuclides present in a sample is traditional gamma ray spectroscopy; one gathers radiation data with a detector having sufficient energy resolution to distinguish the spectral lines due to the various constituents. Typically, one relegates the tedious task of identifying constituent lines to a peak-finding algorithm. This is required when lines merge due to their finite widths. Detailed knowledge of the weighted intensities of measured spectral lines allows one to infer the relative abundance of the sources that contributed them to the spectrum. This approach to measuring the isotopic composition of a sample has been adopted for the Trilateral Initiative and is intended for use in subsequent agreements as well. By coupling these intensities with the detector efficiency and measurement geometry, one may also place a lower limit on the mass of the radiating source. (Lack of knowledge of the surface area and uncertainties in the amount of self-absorption for a concealed source keep this from being a more exact estimate.) Combining the spectral intensities with a knowledge of the decay chains of the sources present gives an estimate of the time elapsed since the sample was prepared or otherwise had some known composition. Subtler aspects of the spectrum, such as the height of continuum relative to key constituent lines, provide information about absorption and scattering due to intervening material. Knowing the relevant cross-sections and the density of likely absorbers gives one a means of bracketing the material thickness. Also, in a neutron-producing source such as plutonium, the presence of other significant elements can be inferred from evidence of their activation products. Clearly, the spectrum contains a wealth of information about the object being measured. Any of

these attributes could be adopted as an element of a material transparency or arms control agreement. Conversely, any attribute not adopted would be considered extraneous and very possibly sensitive.

The role of the information barrier, in cases where gamma spectroscopy is applied as a measurement technique, is to extract and accentuate those attributes of the spectrum chosen for the inspection regime and to conceal all others. This necessarily interposes a layer of automation between the operator and the instrument and largely eliminates human intervention from the inspection process. In normal laboratory measurements, a human experimenter witnesses the accumulation of counts as a sample is measured. He or she looks for telltale peaks to appear and notes the quality of their shapes, while simultaneously monitoring the fraction of detector dead time to ensure that the chosen combination of source intensity, detector solid angle, and count time takes advantage of the full dynamic range of the pulse height analyzer without producing anomalous readings due to pileup or lost counts.

Most attributes do not require information from the full spectrum for their derivation. Specifically, one may calculate the ratio of  $^{240}\text{Pu}$  to  $^{239}\text{Pu}$  using spectral lines bracketed by a narrow subinterval spanning 630 to 670 keV. Figure 2 gives a perspective on the interval of spectral information needed for this calculation.

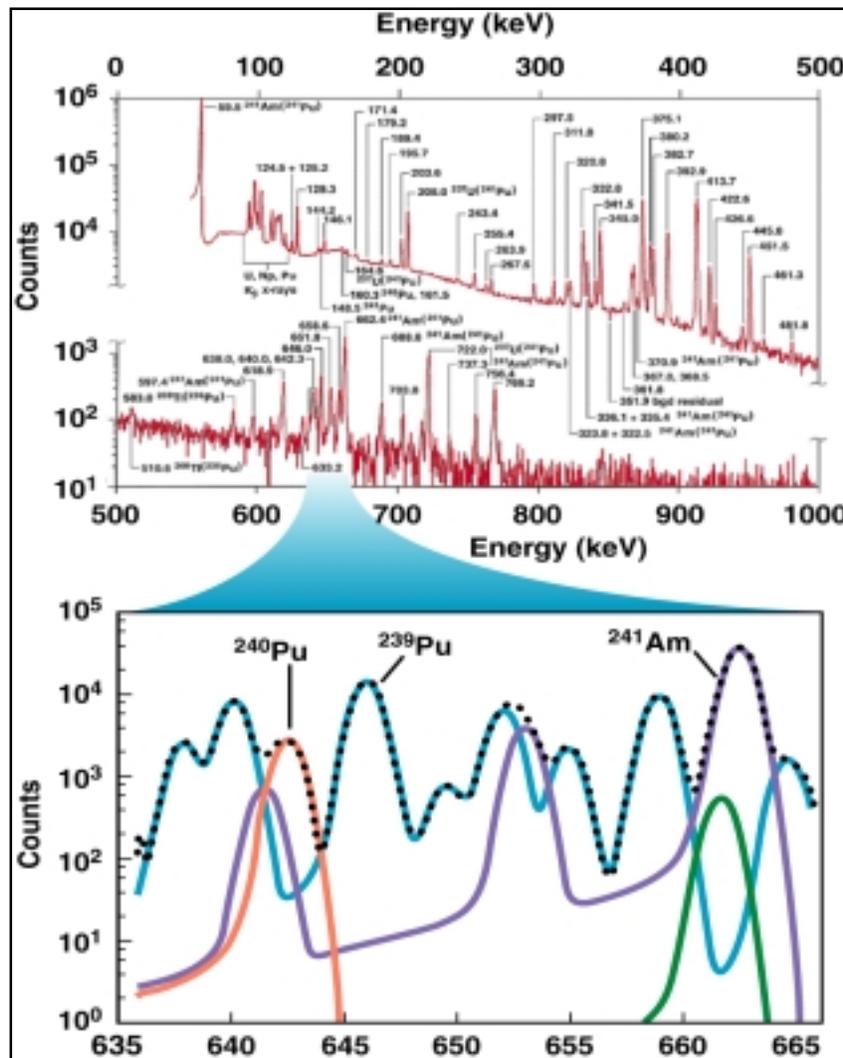


Figure 2. Plot of the gamma ray spectrum from a sample of plutonium containing several isotopes and decay products, showing the relatively narrow subinterval containing the spectral lines used in the Pu600 ratio calculation. Note that since the continuum over this interval is very flat on the scale of the peak magnitudes, no special corrections need be made to account for differential absorption. (Plot courtesy of Thomas B. Gosnell, LLNL.)

This ratio is sufficient to distinguish plutonium suitable for weapons from, for example, that intended for a reactor. (The ratio is a key attribute in the Trilateral Initiative.) Koenig pursued this idea and developed software intended for use in MRI.<sup>7</sup> He built on a more generalized tool created earlier by Gunnink.<sup>8</sup> The tool was named "Pu600" after the range of spectral lines it utilizes. Luke adapted and enhanced Pu600 for the requirements of the Trilateral Initiative.<sup>9</sup> By setting the discrimination values appropriately, the acquisition software limits the data acquired into the pulse height analyzer to this relevant subinterval. This exclusion of unnecessary data at the acquisition stage is only the first layer of a planned "defense-in-depth" approach, which at all successive points along the data flow, retains only the minimum amount of potentially sensitive information needed to calculate the attribute.

The requirement to conceal the spectrum from the inspector eliminates the possibility of direct intervention in optimizing the measurement, and shifts this burden to the instrument and its designers. The gamma ray measurement for the trilateral initiative takes place for a fixed count time and at a prescribed distance from the controlled items. Maintaining data quality and accommodating the full range of source intensities possible under the agreement require an additional measure: an adjustable shield to regulate the count rate in the detector, effectively enlarging and reducing the detector solid angle.

Luke at LLNL solved this problem directly by designing an adjustable diaphragm (iris) with leaves made of tungsten approximately 1 cm thick. The tungsten leaves of the iris move to form an aperture whose size is determined autonomously by the instrument, based on a consideration of the maximum allowable dead time. This ensures good counting statistics, and since the enclosure shrouds both the iris and the detector, the inspector is prevented from estimating the included solid angle of the detector face. Once a source is in place in front of the iris and counting begins, a stepper motor closes the aperture until the count rate matches a preset value. This value assures ample resolution of the spectral features while keeping the detector dead time to a value that preserves the spectral line shape and favors the success of the ratio calculation. Should the iris mechanism lose power, as would normally occur when the shielded enclosure is open for maintenance, then a spring mechanism quickly restores the iris to its fully-open position.

For the security watchdog to protect the measurement data effectively, it must expunge it completely by withdrawing power in case of anomalous events. Therefore the instrument must contain no persistent memory. This places unique requirements on the computer that controls the acquisition and executes the analysis software. In particular, it may contain no fixed magnetic media such as a hard or floppy disk. Thus the boot process must read from some read-only media such as a ROM chip or CD-ROM. Also the processor memory must be volatile and decay quickly when powered down. And, since this process must run without intervention, neither a keyboard nor a display are connected. Its results are communicated via serial interface. White at LLNL has designed and built several such systems for the Trilateral Initiative. They boot MS-DOS from a CD ROM and create RAM disks from which to run the analysis software.

The system depicted in Figure 3 integrates together each of the design elements discussed so far, including the physical barrier, the simplified display, the special purpose computer, and the tungsten iris. The data flow proceeds from left-to-right. Radiation from the controlled item penetrates the shielded enclosure and falls onto the detector through the aperture of the tungsten iris. Counts from the detector accumulate in the multichannel analyzer (MCA). The iris controller operate in parallel with the multichannel analyzer, using a separate analog output line from the detector to monitor the count rate and close the diaphragm as needed. This process is autonomous; the iris controller neither supplies data to nor accepts signals from the computer which controls the detector. In addition to ramping and maintaining the detector bias voltage, the computer sets the measurement parameters, including the range discrimination values, using software written by White. This same software acquires the spectrum subinterval at the conclusion of the measurement. The computer then uses the Pu600 physics software to locate component peaks and calculate the isotopic ratio of  $^{240}\text{Pu}$  to  $^{239}\text{Pu}$ . To this point, all data values are treated as sensitive. Then, the result of this calculation is compared to a threshold, to get a non-sensitive "yes/no" attribute, which passes through the data barrier to the inspector's display. All sensitive data extant in the system are purged prior to the next measurement.

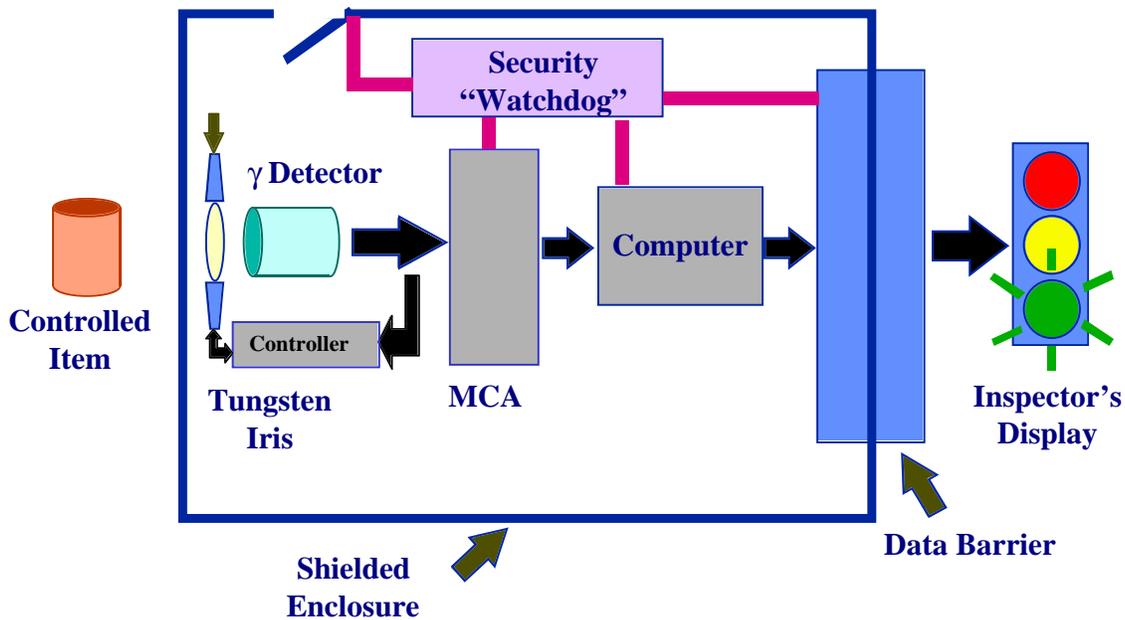


Figure 3. Block diagram of a gamma ray inspection system with an information barrier. The key elements of the information barrier include: (1) an opaque, grounded conducting enclosure, which is essentially a Faraday cage to prevent any telltale EM emanations from the instrument electronics from getting outside; (2) a simple display to give the inspector a yes/no indication of the state of the item being measured. In addition, a "yellow" light might be used to indicate when for any of a set of prescribed reasons, the measurement encountered a nonfatal error; and (3) a "security watchdog" which activates on indications of events which threaten data security, and shuts off power to the internal components, thereby expunging any data remaining there. One example of a triggering event might be the opening of the enclosure during the course of a measurement. Others might be certain classes of internal software error or measurement time-out or hardware ground fault. The data barrier is another component of design element (1). It provides the isolation between the sensitive data volume inside and the external display.

## 7. SUMMARY

The technology of information barriers is primitive compared to the technology of radiation detection and data reduction. Nevertheless, relatively simple systems, such as those described above and in the references, have provided sufficient assurance to sustain negotiations. Indeed, the simplicity of the designs themselves provides confidence in their reliability. The specific implementation of an information barrier system will depend on the requirements of the inspection regime. Nevertheless, the three elements introduced here will always form its basis. More specific design influences include decisions about equipment origin and custody, and the number and type of physical attributes to be collected. Ultimately, the success of such systems will depend on the active participation of the nations or organizations with a stake in the outcome.

## ACKNOWLEDGMENTS

This work was completed by Lawrence Livermore National Laboratory and by Los Alamos National Laboratory for the U.S. Department of Energy under contracts W-7405-ENG-48 and W-7405-ENG-36 respectively.

## REFERENCES

1. Dr. Ray McGuire, private communication.
2. D. J. Mitchell, K. W. Marlow, and H. L. Scott, *Application of a Low-Resolution Gamma-Ray Spectrometer for Nuclear Material Confirmation*, Proceedings of the Trilateral Technical Workshop, December 2-5, 1997, Livermore, California, 26.
3. J. K. Mattingly, J. T. Mihalcz, T. E. Valentine, J. A. Mullins, and S. S. Hughes, *Operational Use of NWIS for Storage of Weapon Components at the Oak Ridge Y-12 Plant*, ORNL Report No. Y/LB-15,943 R2, June 26, 1998.
4. P. Zuhoski, L. Foreman, and P. Vanier, *CIVET - Controlled Intrusiveness Verification Technology*, Brookhaven National Laboratory Internal Report.
5. D. W. MacArthur and R. M. Whiteson, *Functional Requirements for a Prototype Inspection System and Information Barrier for the Trilateral Initiative*, Los Alamos National Laboratory, LA-UR-99-829, February 1999.
6. R. M. Whiteson, D. W. MacArthur, and R. P. Landry, *Functional Specifications for a Prototype Inspection System with Information Barrier*, Los Alamos National Laboratory, LA-UR-99-1174, April 1999.
7. Z. M. Koenig, J. B. Carlson, D. L. Clark, T. B. Gosnell, *Plutonium Gamma-Ray Measurements for Mutual Reciprocal Inspection of Dismantled Nuclear Weapons*, Proceedings of the 35<sup>th</sup> Annual Meeting of the INMM, Vol. 22, 1152 (1995)
8. R. Gunnink, MGA: *A Gamma Ray Spectrum Analysis Code for Determining Plutonium Isotopic Abundances*, Vols 1 and 2, LLNL UCRL-LR-103220 (1990)
9. S. J. Luke, J. B. Carlson, D. L. Clark, T. B. Gosnell, and Z. M. Koenig, *Determining the Ratio of <sup>240</sup>Pu to <sup>239</sup>Pu by High-Resolution Gamma Ray Spectroscopy*, Proceedings of the Trilateral Technical Workshop, December 2-5, 1997, Livermore, California, 22.