International Atomic Energy Agency Use of Facility Calorimeters for Safeguards Purposes

L. P. McRae
C. H. Delegard
R. A. Hamilton
G. A. Westsik
Westinghouse Hanford Company, Richland, Washington, USA

T. F. Moriarty
R. J. Lemaire
International Atomic Energy Agency, Vienna, Austria

Date Published
June 1996

To Be Presented at
INMM 37th Annual Meeting - 1996
July 28 - August 1, 1996
Naples, Florida

Prepared for the U.S. Department of Energy
Assistant Secretary for Environmental Management

Westinghouse Hanford Company
P.O Box 1970
Richland, Washington

Management and Operations Contractor for the
U.S. Department of Energy under Contract DE-AC06-87RL10930

Copyright License: By acceptance of this article, the publisher and/or recipient acknowledges the U.S. Government's right to retain a nonexclusive, royalty-free license in and to any copyright covering this paper.

Approved for public release; distribution is unlimited
International Atomic Energy Agency Use of Facility Calorimeters for Safeguards Purposes
10. LEGENDS/NOTICES/MARKINGS [Required by WHC-CM-3-4 or Reviewed]. Reviewer indicates applicable markings to be affixed or removed.

<table>
<thead>
<tr>
<th>Affix</th>
<th>Remove</th>
<th>Initials</th>
<th>Affix</th>
<th>Remove</th>
<th>Initials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11. MANDATORY COMMENTS (List only mandatory comments here. All other comments shall be made on the document and returned to the author.)

<table>
<thead>
<tr>
<th>Reviewer (Print &amp; Sign)</th>
<th>Date</th>
<th>Resolved by Author/Requestor (Print &amp; Sign)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. ADDITIONAL INFORMATION/COMMENTS:

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
ABSTRACT

The International Atomic Energy Agency (IAEA) is performing nuclear materials safeguards on an inventory of pure and scrap plutonium oxide powder materials held in Vault 3 of the Plutonium Finishing Plant, operated by the Westinghouse Hanford Company for the U.S. Department of Energy at the Hanford Site in Washington State. The IAEA uses weighing, sampling, and destructive analyses to obtain the most accurate verification measurements of containers of plutonium powders.

In contrast, the plant operator generally uses non-destructive plutonium assay based on gamma spectrometry and calorimetry for its most accurate plutonium powder container measurements. Recent results have shown that the operator's calorimeter system achieves measurement variabilities comparable with, or better than, the destructive analyses, particularly for scrap. The results are achieved more quickly and economically, with less waste and lower radiation exposure and contamination hazard, by calorimetry than by classical destructive analyses.

Techniques, including authentication methods, are being jointly developed to permit use of the operator's calorimeter system for international safeguards purposes. The authentication is to ensure the independence of, and to substantiate the validity of, calorimeter measurements for international safeguards. The authentication methods considered and being developed are discussed.

INTRODUCTION

The International Atomic Energy Agency (IAEA) conducts nuclear materials safeguards on an inventory, held in Vault 3 in the 2736-Z Building of the Plutonium Finishing Plant (PFP), of about 1,000 items containing plutonium oxide powder. The PFP is operated by Westinghouse Hanford Company (WHC) for the U.S. Department of Energy (USDOE) at the Hanford Site in Washington State.

The plutonium, which originated from the U.S. nuclear weapons complex, includes relatively pure plutonium oxide (PuO₂) powders as well as impure plutonium-bearing scrap materials arising from a number of processes (Welsh et al.'). The plutonium is packaged in nested sets of three metal cans with the plutonium powders, ranging in net mass from 200 to 2,000 grams, contained in the innermost can.

The International Atomic Energy Agency uses qualitative and quantitative techniques to verify the presence and quantity of the nuclear materials under safeguards. The Agency uses weighing, sampling, and destructive analyses to obtain the most accurate verification measurements of containers of plutonium powders.
The contributions of material heterogeneity to the total DA analytical error also were determined. The variabilities of the plutonium measurements obtained by the PFP were compared with results obtained in IAEA safeguards experience and with international target values (Welsh et al.).

The comparison, shown in the Table, indicates that for impure (scrap) items, the coupled calorimetry and gamma NDA results give lower variability than the results obtained by weighing, sampling, and DA. Even for pure (product-quality) PuO₂, the combined calorimeter and gamma NDA results are only slightly inferior to the results obtained by quantitative DA methods. The relative success of calorimetry/gamma NDA is possible because the NDA gamma measurements greatly reduce, and calorimetry totally avoids, the sampling variability (manifest as random error) and interferences associated with DA.

The sampling, shipping, analysis, and waste disposal operations required for DA are costly in time, money, and radiation exposure for both the IAEA and the PFP operator. These considerations, and the comparative analytical findings (Welsh et al.), persuaded the IAEA to consider the possibility of replacing part of their quantitative destructive analysis requirements with shared IAEA use of installed PFP calorimeters.

Under the proposed shared use, the calorimeter measurements (in conjunction with gamma spectrometric NDA performed by existing IAEA instrumentation and methods to determine plutonium isotopic composition) must demonstrate accuracies and precisions competitive with those achieved by IAEA's sampling, weighing, and DA. Equally important, the IAEA must be able to authenticate the use of the calorimeter results to draw valid safeguards conclusions. Detailed steps in the practical implementation of IAEA use of the PFP equipment also must be created to provide containment and surveillance (C/S) and computer security during and between measurement operations.

This paper provides an evaluation of methods the system operator (including agents of the United States government) could use to provide falsified calorimeter results to the IAEA for purposes of nuclear material diversion, and describes measures the IAEA could take to detect (and thus deter by risk of detection) the presentation of false calorimeter data and gain assurance in the reliability of calorimeter data provided by the PFP equipment for IAEA-selected items.

**AUTHENTICATION APPROACHES**

Several approaches the IAEA could take to assure independent and authenticated use of the operator's calorimetry system were considered. Included in these approaches were self-protecting characteristics of the calorimetry measurement system and various C/S and computer security measures that make tampering detectable by IAEA inspectors. The approaches considered were:

1. performance authentication by DA
2. hardware/software design information verification complemented by C/S
3. standards measurement complemented by C/S
4. performance authentication by blind power-source spiking
5. performance authentication by blind item loading and power-source spiking.

**Performance Authentication by Destructive Analysis**

In performance authentication by destructive analysis, the IAEA inspector would exercise the right to select, at random, items for bias verification by weighing, sampling, and DA. By employing this right for items already measured by the calorimeter, the inspector could validate the performance of the calorimeter and thus the results provided by the operator. The operator providing false calorimeter results would suffer the risk of detection. The inspect thus could ensure that calorimeter results provided by the operator were trustworthy if the calorimeter results and DA results for the corresponding selected items were in agreement.

A plausible diverter's strategy would be to operate the calorimeter to give measurement results that simply mirrored the declared falsified values (within some minor fluctuation so that the declared and measured values did not match exactly). The calorimeter measurements provided by the operator thus would become a reiteration of the measured items' inventory listing. A benefit from the diverter's view would be that no "flyers" showing significantly different declared and measured values would exist. Given the possibility that the operator might use this strategy, however, the IAEA could not give credence to any calorimeter result.
TABLE. MEASUREMENT VARIABILITY ESTIMATES

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Variability Estimates, % Relative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PFP Experience(^a) Random/Systematic</td>
</tr>
<tr>
<td></td>
<td>&quot;Pure&quot; PuO(_2)</td>
</tr>
<tr>
<td>Weigh/Sample/DA</td>
<td>0.2/0.1</td>
</tr>
<tr>
<td>Calorimetry</td>
<td>0.34/0.1</td>
</tr>
</tbody>
</table>

\(^a\) Welsh et al.\(^1\).
\(^b\) Average over all facilities.
\(^c\) ITV is International Target Values, Deron et al.\(^2\).
\(^d\) Plutonium-uranium mixed oxides.

To counter this strategy and detect the diversion of the goal quantity by bias defects, the IAEA therefore would be required to verify the same number of items by weighing, sampling, and DA as would be required in the absence of calorimetry. Though DA validation of calorimetry initially appears attractive, further consideration shows that, by itself, adoption of performance authentication by DA represents no improvement over the existing IAEA bias defect verification approach of weighing, sampling, and DA.\(^*\)

Design Information Verification and Containment/Surveillance

Exhaustive design information verification of the calorimeters may be employed to accept WHC calorimeters for IAEA use. To maintain continuity of knowledge of the verified equipment, the IAEA would apply appropriate C/S devices.

In considering this option, possible ways the operator might falsify the calorimeter output (readings of item power production) through hardware and software manipulations must be considered. Measures the IAEA might take to detect the falsifications then must be devised. The design verification approach clearly requires intimate IAEA familiarity with the construction, operation, and software associated with the PFP calorimeters.

To counter software falsifications, the IAEA must be able to validate and use its own computer/controller and associated software. To counter hardware tampering, the IAEA also must guarantee a high level of oversight and control of the surroundings of the calorimeters. For example, a number of tamper-indicating enclosures (on the item measurement cavity, on the standard resistor, on cabling junction boxes, and sheathing on the cabling itself) must be devised. Enclosure boxes must be secured by IAEA seals. Console equipment that cannot be enclosed due to heat loading, but which is physically accessible for tampering, must be left under visual inspector surveillance or placed under video surveillance with short interval times during the actual measurements.

Unless continuous and conclusive C/S were maintained between IAEA operation periods, extensive re-verification of the calorimeter design would be required before the equipment could be re-used by the IAEA. Review of short-interval surveillance records likely would be inconclusive due to legitimate operational activities around the calorimeters. A comprehensive design verification approach clearly would require a large IAEA effort.

\(^*\) The IAEA uses sampling and DA confirmation to accept verification results obtained from equipment installed in a reprocessing plant under IAEA safeguards (Franssen et al.\(^4\)). Plutonium product solution concentration verifications by K-edge densitometry satisfy a large fraction of the IAEA bias verification requirements for this inventory stratum. The K-edge findings are substantiated by DA verifications of a selected subset of the product batches. Unlike the PFP calorimeter, however, the K-edge instrument is IAEA equipment and not under operator control.
Measurement of Standards and Containment/Surveillance

Measurement of standard items, complemented by C/S measures, were considered to overcome certain of the difficulties associated with the calorimeter design verification. This approach would consist of measurements of inventory items previously verified by IAEA DA and successfully kept, since verification, under IAEA C/S. Following measurement of selected standard items, IAEA verification measurements on the calorimeter could be conducted.

However, as in the design authentication approach, measures against introduction of spurious signals to the calorimeter hardware still would be required. This would necessitate the same scope of C/S measures during the inspection measurements as required for the design information verification approach. Similarly, the IAEA would still need to regulate calorimeter operation through a validated computer/controller and associated software. The IAEA also would have to guard against introduction of spurious power sources into the calorimeter well.

Despite the perceived attractiveness of this method over the design verification approach, clandestine signal generation devices could still exist in the hardware to supply false information to the IAEA computer/controller. The IAEA then would have to conduct design verification to detect such hardware tampering. In the end, it was judged that this option, by itself, would not be sufficiently robust to provide assurance to the IAEA of reliable calorimeter data.

Performance Authentication by Blind Power-Source Spiking

Discussions of the DA confirmation, design verification, and standards measurement approaches showed that the fundamental difficulty with IAEA use of any operator-owned and -maintained equipment is the extensive control and accessibility the operator enjoys over that equipment. To use the operator’s equipment with confidence, the IAEA must either:

• become as skilled and familiar as the operator in the equipment operation and be able to authenticate the equipment design each time the equipment is used for IAEA measurements; or,

• independently introduce a discrete and known factor into the verification measurement that the operator cannot know or control.

Blind (to the operator) power-source spiking of items being measured by calorimetry was considered as a possible approach to introduce an aspect of independent IAEA control to the calorimeter verification measurements. This approach would entail measurement of the combined power arising from an inventory item selected for verification and from 239Pu or electrothermal sources added by the IAEA inspector. The power added by the IAEA would be unknown, \textit{a priori}, by the operator. To give latitude in the amount of thermal power added, a number of 239Pu spikes would be required. If electrothermal power sources were used, one source would be required for each operating calorimeter. Both 239Pu and electrothermal sources have been used in plutonium assay calorimetry (Otto 5).

Based on the calorimeter measurement, the power output of the selected item plus added power spikes would be reported to the inspector by the operator. The inspector would subtract the power contribution due to the known added power and derive, by difference, the power due to the inventory item.

The operator could not know the magnitude of the added spike power until the end of the measurement (when the amount could be calculated by difference based on the amount of power provided by the known inventory item). At this point, the operator could, in theory, still tailor the calorimeter output at the end of the measurement to give a falsified result that would match a falsified item inventory declaration.

Blind power-source spiking, therefore, still has the shortcomings that the operator knows the identity of the item being measured and controls the measurement system. With this knowledge and control, the operator could falsify the measurement to give a desired result to match a falsified inventory statement.

Performance Authentication by Blind Item Loading and Power-Source Spiking

If the IAEA inspector knew, but the operator did not know, which item was being measured, the inspector alone would control a key parameter of the measurement. The operator, therefore, would not be able to falsify the calorimeter power result with confidence to give a specific (falsified) value. The IAEA could gain this knowledge by controlling the item loading into the calorimeter (or into the sample adapter that contains the item to be measured). This authentication measure is called...
blind item loading because the identity of the item being introduced to the calorimeter would be blind to the operator.

In practice, such an arrangement could be accomplished by the IAEA if the inspector had on hand at least two items from which an item to be measured could be selected. With proper concealment arrangements (e.g., an otherwise windowless glovebox with a small IAEA-controlled viewing port), the operator would introduce the selected item "blindly" into the measurement adapter outside his view or the views of other operators. The remaining item(s) would be kept in IAEA-sealed overpacks or enclosures to retain IAEA’s privileged knowledge of the identity of the item being measured. To obscure further from the operator the measured item’s identity (which could be determined by calorimeter measurement of the thermal power arising from the item), the inspector also could use power-source spiking, as described in the previous section.

The operator then would measure the item-plus–spike power by calorimetry and report the results to the inspector. The inspector could determine the power due to the inventory item by difference and proceed with the next measurement. To guarantee that the operator could not anticipate which item was being measured, the IAEA inspector would always require at least two inventory items to be available from which one would be chosen, blind to the operator, for measurement.

Assessments of the blind item loading and power-source spiking approach were performed. By one evaluation, it was argued that the potential diverter has the possibility to learn, to high accuracy, the thermal power values (wattages) of the individual spike sources even if the sources were obtained from an unknown supplier. This is because the number of $^{238}$Pu sources is necessarily limited; a database of calorimeter measurements of combined items and spikes could be gathered over time by the operator. With knowledge of the thermal power values of the spikes, and the knowledge of the thermal power values for the several items available for measurement, the possible permutations of total power (items plus spike(s)) could be readily calculated. Thermal power spiking would be resistant to this diversion scenario if the infinitely-variable electrothermal power spikes were used instead of the discretely-valued $^{239}$Pu power spikes.

Design and capital costs of the necessary electrothermal power devices and various "blind-loading" mechanisms also were examined. All required custom designs and high levels of oversight for use with special nuclear material. The electrothermal devices also required integration into the sample adapters and certifiable accuracy. As a result, estimated costs to procure and maintain this hardware are relatively high.

Finally, the assessment showed that the clandestine use of electronic tags by the operator is a possible vulnerability of any blinding technique. The tags are small and emit a radio signal that uniquely identifies the device. If a tag were concealed in an inventory item, the sample adapter, even if blind-loaded, could be interrogated surreptitiously and the identity of the item determined by the operator. Tests with various electronic tags showed this vulnerability does, in fact, exist.

SELECTED APPROACHES

No single approach was judged to be totally satisfactory for routine IAEA use. Each approach, however, had attractive elements. Combination of certain of these elements can provide a high degree of assurance that reliable calorimeter measurements may be obtained for IAEA purposes from operator equipment. The measures selected for acceptance testing are:

- DA sampling and analysis of selected items following their calorimeter measurement
- demountable IAEA-controlled hard drive for the calorimeter computer operation
- IAEA use of IAEA-authenticated calorimeter software; keyboard password lockout
- sealing of access to the calorimeter sample adapter well during measurement of items for IAEA verification
- calorimeter measurement of selected items (standards) previously verified by IAEA DA.

In considering the design verifications, it was recognized that IAEA ownership of the calorimeter operational software and access to real-time measurement performance data (e.g., temperatures,
The power-source spiking and blind item loading authentication approaches were judged to be too cumbersome and expensive to implement and maintain for routine IAEA use. The spiking and item blinding concepts may be applicable, however, in other situations. It was judged that the combination of the five measures (DA checking, standards measurement, IAEA hard drive, software validation, and sealing), used in concert with the existing safeguards verification techniques, attain an achievable balance in credibility and practicality for PFP calorimeter authentication.

Acceptance testing and training of IAEA personnel on the PFP calorimeter systems is underway. Acquisition of the computer hardware and authentication of calorimeter software is also in progress.

ACKNOWLEDGEMENTS

Tests with electronic tags were conducted by Ivan Waddoups and Pete Bortniak of Sandia National Laboratory. This work is being sponsored by the Program of Technical Assistance to Agency Safeguards (POTAS) of the International Safeguards Program Office, Brookhaven National Laboratory.

REFERENCES


