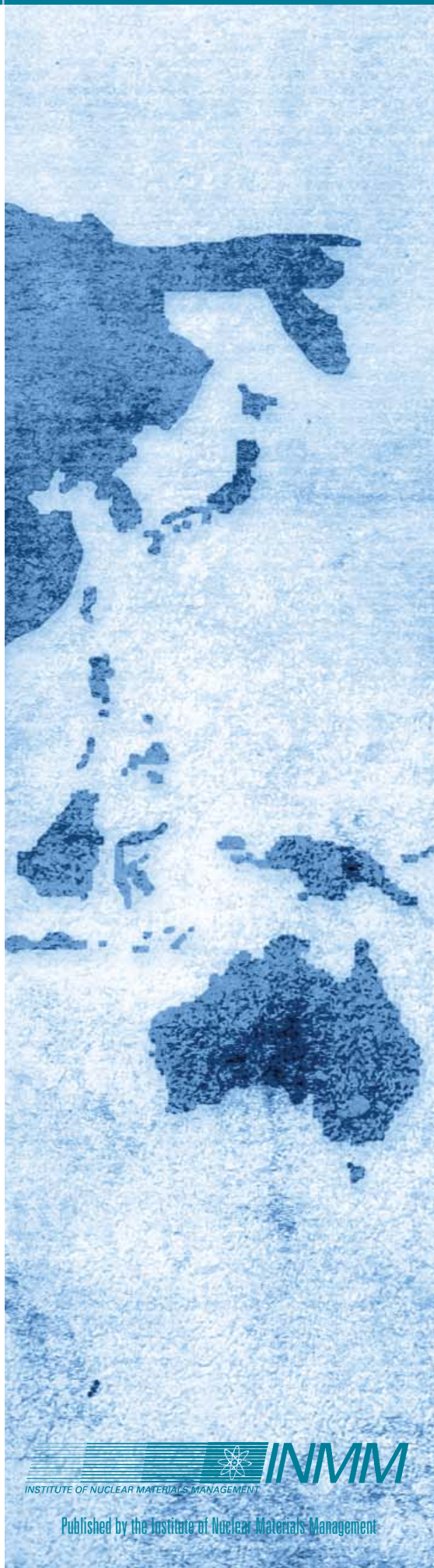
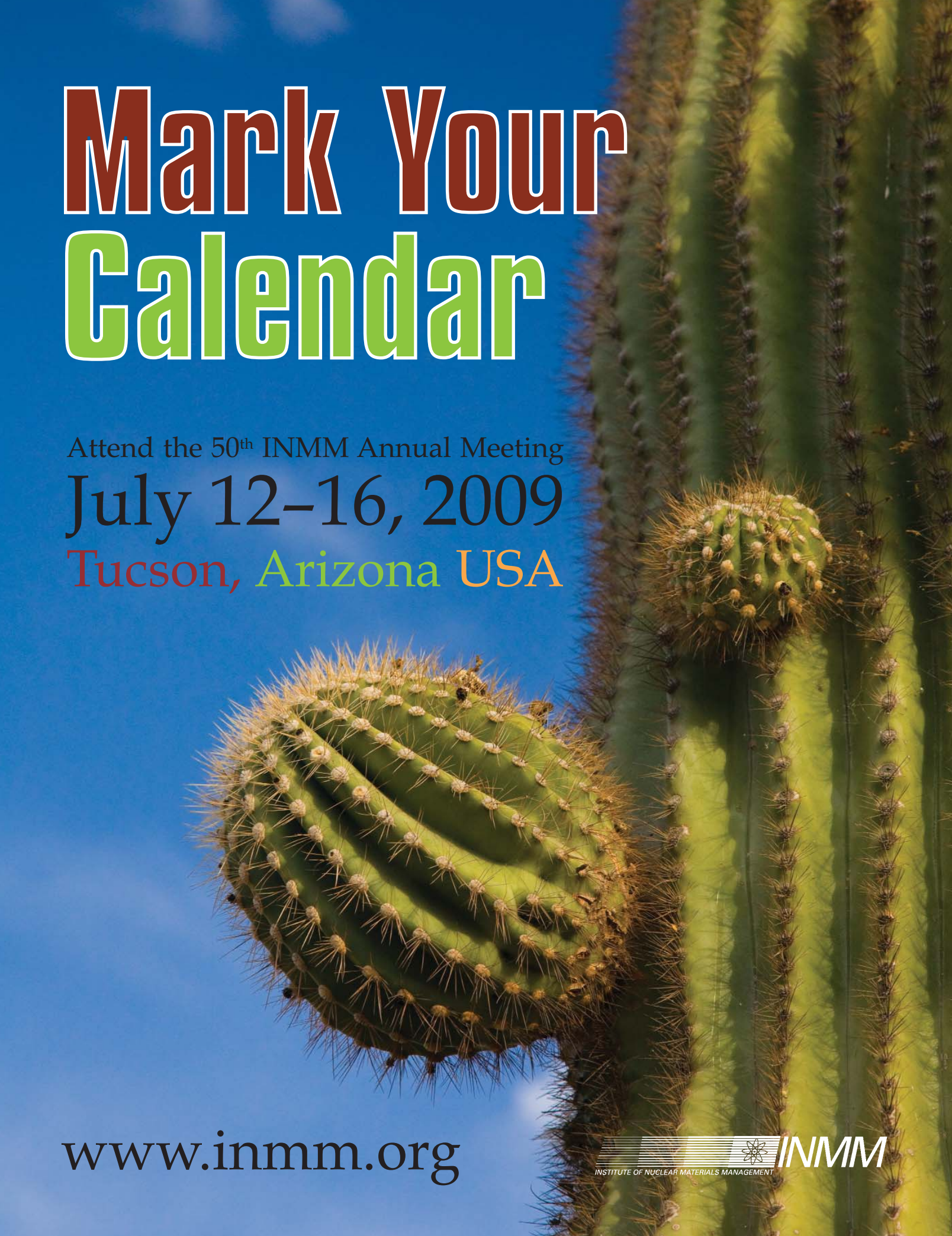
Fall 2008 | Winter 2009 | Spring 2009 | Summer 2009 | Volume XXXVII, Number 1

JNMM Journal of Nuclear Materials Management



INMM
INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT
Published by the Institute of Nuclear Materials Management


Mark Your Calendar
Attend the 50th INMM Annual Meeting
July 12–16, 2009
Tucson, Arizona USA
www.inmm.org
INMM
INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT

JNMM Journal of Nuclear Materials Management

JNMM (ISSN 0893-6188) is published four times a year by the Institute of Nuclear Materials Management Inc., a not-for-profit membership organization with the purpose of advancing and promoting efficient management of nuclear materials.

SUBSCRIPTION RATES: Annual (United States, Canada, and Mexico) $200.00; annual (other countries) $270 (shipped via air mail printed matter); single copy regular issues (United States and other countries) $55; single copy of the proceedings of the Annual Meeting (United States and other countries) $175. Mail subscription requests to *JNMM*, 111 Deer Lake Road, Suite 100, Deerfield, IL 60015 U.S.A. Make checks payable to INMM.

ADVERTISING, distribution, and delivery inquiries should be directed to *JNMM*, 111 Deer Lake Road, Suite 100, Deerfield, IL 60015 U.S.A., or contact Jill Hronek at +1-847-480-9573; fax, 847/480-9282; or E-mail, inmm@inmm.org. Allow eight weeks for a change of address to be implemented.

JNMM Journal of Nuclear Materials Management
Winter 2009, Volume XXXVII, No. 2

Topical Papers

Institute News

Departments

INMM
INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT

Is the Nuclear Renaissance Real?

By Steve Oritz
INMM President

A lot of discussion lately cites the beginning of a nuclear renaissance. It is clear that world energy demand will continue to grow. It will become increasingly difficult to meet this demand with fossil fuels. At this year's General Conference of the International Atomic Energy Agency, a consistent theme was renewed interest in building nuclear power reactors. Many countries are pursuing aggressive programs to add more nuclear reactors as a source of peaceful energy. Other countries are looking into building their first nuclear reactors.

The growth in nuclear energy will lead to the need for more nuclear material managers. We will see a greater need for professionals focused in the six technical divisions of the Institute of Nuclear Materials Management. We as an institute are beginning to realize the renewed interest in nuclear material management. We have approved the petition of three student chapters since our annual meeting in July. We have also approved the petition of a new chapter from the United Kingdom. Unlike many professional societies, INMM crosscuts many technical disciplines. We are made up of professionals from engineering, sciences, business, and law. What brings us together is the focus on nuclear materials management.

Challenges

Along with the increase of nuclear as an energy source come many challenges. We still need to provide safe and secure transportation of nuclear material. We still need to provide safe and secure waste management. We still need to provide physical security of our nuclear reactors and material at fixed sites. We still need to ensure nonproliferation. We still need to provide strict control and accountability of nuclear materials. And as a global community we must continue to share best practices in all these areas of nuclear materials management. If we fail in any of these areas the results could be disastrous. It is professionals like us who will make sure we provide a safe and secure environment for nuclear materials management.

Student Chapters

The Institute is experiencing a growth in the number of student chapters. Student chapters have only been in existence as part of the Institute for a few years. The first chapter was Texas A&M. This chapter has demonstrated a strong relationship with the Southwest Regional Chapter since its inception. It is vitally important that regional chapters develop a relationship with the student chapters in their area. This will provide a level of mentorship and connectivity necessary to nurture young professionals interested in nuclear material management. The success of our student chapters will feed the success of the Institute of Nuclear Materials Management. Current student chapters of INMM are Texas A&M, Mercyhurst College, University of Missouri, University of Michigan, and University of Tennessee.

World Institute for Nuclear Security (WINS)

The official standup of WINS occurred in September 2008 at the General Conference of the International Atomic Energy Agency (IAEA). INMM Immediate Past President Nancy Jo Nicholas gave a short speech at the launch ceremony for WINS. Other participants at the ceremony were IAEA Director General Mohamed ElBaradei, U.S. Secretary of Energy Samuel W. Bodman, former U.S. Senator and, Nuclear Threat Initiative (NTI) Co-Chair Sam Nunn and NTI President and Chief Operating Officer Charles B. Curtis. INMM is currently looking at how best to support WINS in the future.

INMM President, Steve Ortiz can be contacted by e-mail at sortiz@sandia.gov.

Reflections on INMM's Fifty Years

By Dennis Mangan
Technical Editor

As I reflect on the Institute's fifty-year history and accomplishments, it is a pleasure to reflect on our growth. I can recall when we had annual meetings in smaller hotels and didn't have consecutive sessions, particularly six or seven. I also reflect on the growth of the *Journal* over the years. I can remember the *Journal* when its technical editors were Willie Higinbotham of Brookhaven National Laboratory (from the mid 1980s till the mid 1990s) and Darryl Smith of Las Alamos National Laboratory (from the mid 1990s till the late 1990s). I was honored to succeed these talented gentlemen in the late 1990s. Early on in my shift, I thought it would be interesting for our members to find newsworthy articles (e.g., technical division reports, committee reports, etc that were provided to the Executive Committee of the Institute at its three EC meetings throughout the year) in the *Journal*. I recall a goal that I had which was to have a report from every one of our divisions/committees in a *Journal* issue. I never reached that goal. In fact, with the advent of Web sites and the desire of the Executive Committee to broaden the INMM Web site (www.inmm.com), a positive decision was made several years ago by the EC to place information about the divisions and committees on the Web site behind the "members only" section. What has evolved is a quality and professional INMM Communicator. I encourage all INMM members to visit that site and read the information provided in the Communicator by various key INMM individuals.

An interesting contribution is by our vice presentment, who provides a timely report of our EC meetings. There are also topical reports by authors who have attended various meetings of interest. It's an enjoyable site to visit. The impact on the *Journal* by the EC to inaugurate the Communicator was likewise positive. We turned our attention to mostly technical articles (except for our fall issue, which reports on the INMM Annual Meeting) and we further developed a peer-review process for published articles. This peer-review process, coordinated by our assistant editor with cooperation from our associate technical division editors and our managing editor, has evolved over the years to greatly assist the quality of our published articles. We likewise have been able to get our past Journals on the inmm.com website with a search engine that allows members to quickly find articles of interest. These are just of few of my recollections of growth over our fifty-year history.

In this issue of the Journal we have three diverse and interesting articles. The first, *Verifying Sensitive Parameters Without Measuring Sensitive Values,* is authored by Jonathan Sanborn of the U.S. Department of State. Sanborn addresses an extremely difficult problem: if in the course of verifying a treaty or agreement a sensitive parameter needs to be verified, how can the inspecting state or organization satisfy meeting the requirement without obtaining specific sensitive information during the verification measurement process. He presents interesting and logical approaches. The second paper, *Contact Memory Buttons and Nuclear Safeguards,* authored by Jon Warner and Roger Johnston of the Argonne National Laboratory in Argonne, Illinois, USA, cautions the reader to be careful in using tamper-vulnerable inventory control tags for applications that require secure, tamper resistant tags. Their focus is on commercially "contact memory buttons." The third article, *Hypothesis Testing: Frequentist Versus Bayesian With Examples from Nuclear Safeguards* by Tom Burr of Los Alamos National Laboratory in Los Alamos, New Mexico, USA, and Dennis Weier of Pacific Northwest National Laboratory, Richland, Washington, USA, will delight the statisticians in our readership. The examples they study are quite interesting and real world examples

In addition to these three articles, we have a book review by *JNMM* Book Review Editor Walter Kane of Brookhaven National Laboratory. Kane reviews *Deliberative Democracy for the Future: The Case of Nuclear Waste Management in Canada* by Genevieve Fuji Johnson of the University of Toronto, Canada. Also, in commemoration of our fiftieth anniversary, we have an interesting piece by John Lemming titled A Note from a Past President. Lemming was president (then known as chair) of our Institute in 1999 and 1990.

Our congratulations go to *JNMM* Assistant Technical Editor Steve Dupree for being honored with the 2008 A. M. Pate, Jr. Award in Civil War History by the Fort Worth Civil War Round Table for his book, *Planting the Union Flag in Texas: The Campaigns of Major General Nathaniel P. Banks in the West.* This is the second honor Steve received this year. He was also named a Fellow of the Institute at last summer's 49th INMM Annual Meeting in July.

I trust you find this issue of the Journal informative and interesting reading. Should you have any questions or comments, please feel free to contact me.

JNMM *Technical Editor Dennis L. Mangan may be reached via e-mail at dennismangan@comcast.net.*

Verifying Sensitive Parameters Without Measuring Sensitive Values

Jonathan Sanborn
U.S. Department of State, Washington, DC USA

Note: The work reflected in this paper does not purport to represent the views of the U.S. government.

Abstract

A method is presented for verifying arms control agreement conditions relating to objects that the inspected party regards as sensitive. The problem is to verify the condition without revealing anything more about a sensitive parameter; for example, verifying that the weight of an object exceeds a particular value without revealing anything more about the weight. In the approach presented, the object is measured in combination with unknown values. Mathematical models are presented for which it is shown that the treaty condition can be verified in a manner consistent with a rigorously defined requirement that no additional information regarding the sensitive parameter is revealed. Not all verification situations have such solutions; the mathematical conditions required for solutions are identified, and a set of equations for calculating the unknown values is presented. It is then shown how some of the limitations can be overcome with a more elaborate, probabilistic approach.

1. Introduction

Measurements of sensitive items made in the context of verifying a nonproliferation or arms control regime have the potential to cause the acquisition by the measurement instrument of sensitive or classified data. When the physical characteristic of the sensitive object that must be verified is not itself sensitive, then the measurement system can simply be designed to acquire information only on that characteristic. The more difficult problem is one in which some limited amount of information, but no more, must be gained about a parameter that is sensitive. For example, it is desired to verify that the weight of an object exceeds some threshold, without revealing anything else about the weight.

One approach to this problem is to design an instrument that acquires sensitive data, but displays only the information needed; this requires a so-called "information barrier" to prevent the acquired data from being observed. In this case both sides must establish confidence in the functioning of the instrument: the inspecting side must be assured that it performs the specific measurement accurately and reliably, and the inspected side must be assured that it cannot in any way retain or transmit sensitive data to the inspector. Providing this simultaneous assurance in an instrument that depends on modern electronics and software that may be both complex and proprietary may be difficult.

An alternative approach is to present to the instrument the sensitive object in combination with unknowns, so that the instrument never sees sensitive data. A set of measurements must be arranged so that an inference can be drawn that the sensitive parameter fulfills the treaty condition but that *no additional information* can be gained about the sensitive parameter. The basic idea can be illustrated with an almost trivial example. If it is desired to demonstrate that the weight (x) of some sensitive item is less than some value L, the sensitive item can be put on a scale together with a weight whose value (which is chosen as L – x) is unknown to the inspector. The inspector observes that the total weight on the scale is L, and therefore the value of x must be less than L. The weight seen by the scale, L, is not sensitive.[1]

The paper discusses two approaches to this problem: a basic method and an enhanced, probabilistic method. Section 2 describes the requirements for solving a verification problem using the basic approach. Sections 3 and 4 provide examples. Section 5 discusses the issue of when the basic method works, and how to compute the values of the unknowns. Section 6 introduces a probabilistic procedure that extends the set of conditions under which the approach will work. The appendix provides a rigorous and more general mathematical treatment of the problem, including formal definitions of the concepts. A basic theorem identifies when solutions to the basic verification problem exist.

2. Requirements for the Basic Approach

The objective is to verify the truth of a compliance condition, which can presumably be expressed as some sort of mathematical equation or inequality containing the sensitive parameter value and other measured values. This is to be achieved by a measurement procedure yielding observed values that will satisfy certain conditions if the compliance condition is satisfied (defined as *success*), or will not satisfy those conditions if the compliance condition is not satisfied (*failure*). The information gained about the sensitive parameter in this process should be limited strictly to the

fact that it satisfies the compliance condition. In order for this limitation to hold, the data observed by the inspector must depend upon the sensitive value in a specific manner:

(1) Any *conforming* value of the sensitive parameter must yield *the same* observed values as any other conforming value; in this case the procedure should succeed.
(2) If the sensitive value *does not* conform to the compliance condition, the procedure must fail.

Whether the observed data depends on non-conforming values in some way is not considered a concern. The first condition means no information loss and no false alarm for the case of compliance; the second means "100 percent detection probability" in the case of non-compliance.

3. Example with a Sensitive Weight

Consider an object whose weight x is sensitive. We wish to verify that the weight lies between a lower limit L_1 and an upper limit L_2, without revealing any additional information about x. Clearly L_2 and L_1 are not sensitive, and do not depend on x.

The proposed procedure is as follows. The inspected party prepares two weights u_1 and u_2 whose values are $u_1 = x - L_1$ and $u_2 = L_2 - x$ (how these equations are chosen is discussed in section 6). These objects are shown to the inspector (labeled, so the inspector knows which is which, but the inspector *does not know their weights*). Two measurements are made. First, the objects x and u_2 are placed on a scale *together*. The result should be the value L_2. The objects u_1 and u_2 are then placed on a scale *together*. The result should be $L_2 - L_1$. The equations for this system are therefore as follows:

The observations are (the inspector knows this is true as he can observe the weighing, and inspect, or supply, the scale)

$$o_1 = x + u_2 \quad (3.1)$$
$$o_2 = u_1 + u_2 \quad (3.2)$$

The compliance condition is (this is presumably stated in the agreement)

$$L_2 > x > L_1 \quad (3.3)$$

The rules for establishing the values of the unknowns are[2]

$$u_1 = x - L_1 \quad (3.4)$$
$$u_2 = L_2 - x \quad (3.5)$$

It is also known that

$$u_1 > 0 \quad (3.6)$$
$$u_2 > 0 \quad (3.7)$$

The inspector through observation (3.1) confirms the equation $x + u_2 = L_2$ (the observed value is L_2 because of 3.5); and through the observation (3.2) confirms the equation $u_1 + u_2 = L_2 - L_1$ (because of 3.4 and 3.5). Subtracting the second equation from the first gives $x - u_1 = L_1$. Since the weights u_1 and u_2 can be assumed not to be negative the two equations $x + u_2 = L_2$ and $x - u_1 = L_1$ imply that $L_2 > x > L_1$.

Clearly the inspected party would not be able to perform this procedure if the compliance condition were not true; it would involve negative weights. On the other hand if the compliance condition is fulfilled, the data observed by the inspector are the values L_1 and $L_2 - L_1$, and these will be observed whatever the value of x is. Thus this procedure satisfies the conditions stated above.

A Note on the Example

The underlying principle is that we have two measurements and three unknowns (u_1, u_2, and x); the value of x therefore cannot be computed from the equations. This is not the whole story, however; it does not in itself guarantee that some information about x cannot exist in the observed values, or that the observations will serve to verify compliance. The "verification problem" posed in this paper is: given a mathematical model of the set of measurements, can one determine the manner in which the unknowns are chosen so that these objectives are fulfilled. Whether this can be done is not obvious. In fact, if the problem is changed slightly, it seems clear that it becomes intractable. Specifically, if we substitute

$x > L$
for the condition
$L_2 > x > L_1$

a solution in the sense of this paper appears to be impossible. This can be seen from the fact that as soon as a value $x + u_2$ is observed, it is clear that any value for x greater than this observed value is ruled out; and the inspector has thus information about x that he did not have before.

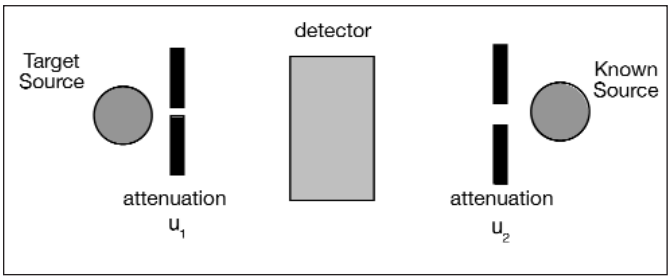
4. Example with a Sensitive Isotopic Ratio

It is desired to confirm that a plutonium isotopic ratio (e.g., the 240/239 ratio) exceeds some threshold L_o, without revealing anything more about that ratio.

Consider an idealized gamma spectrometry instrument, which counts in one channel the number of photons of a particular energy characteristic of Pu-239, and in another channel those characteristic of Pu-240.[3] The detector can be arranged to be exposed to radiation from two sources, and it can be shielded from any source. The situation is illustrated in Figure 1. It is assumed that the physical arrangements can be made transparent enough to the inspector and inspected party that each side can confirm for themselves which sources of radiation are impinging on the detector.

The mathematics of the measurement model below may obscure the underlying principle, which is in fact quite simple. Equations 4.8 and 4.9 indicate that in the solution derived, the sensor effectively sees radiation emitted from a combined source whose isotopic ratio is L_o. Since this source is a mixture of two components, one of which is known to have a lower isotopic ratio than L_o, it is clear that the other component must have a higher ratio to compensate.

Figure 1



The sources arranged around the detector are the target object to be verified, with 240/239 ratio x and a known standard source which has ratio L. It is desired to demonstrate that the isotopic ratio of the target source is greater than some value L_o. In this scheme the unknowns are the attenuations produced by interposing shielding of some sort between the sources and the detectors. These are set by the inspectee.

We will use the following notation and model for this system:

- The known source has isotopic ratio L that is less than L_o. The inspector can verify the value of L, which is not sensitive.
- The isotopic ratio for the target source is x, which is sensitive.
- I_1 and I_2 will denote the count rates that would occur in the detector in the 239 channel due to the target and known source respectively in the absence of the attenuators. The count rates in the 240 channel are modeled as I_1Kx and I_2KL, where K is a physical constant that is assumed to be known, or can be estimated through calibration.[4]
- u_1 and u_2 are the attenuations produced in these count rates because of the shielding.
- o_1 and o_2 are the observed 239 and 240 count rates in the two channels of the detector.
- The symbol $R(x)$ will stand for the ratio $(L_o - L)/(x - L)$. It is clear that $R(x)$ will have a value between zero and one if and only if the treaty condition holds.
- A count rate value of $C < min\ (I_1, I_2)$ is a count rate chosen as the count rate that will be observed in the 239 channel. This value is determined simply on the basis of experimental convenience as within the range of the detector; the sides agree on this value and it is not sensitive.[5]

The values of the attenuators are set as follows: $u_1 = CR(x)/I_1$ and $u_2 = C(1 - R(x))/I_2$. The compliance test will be said to succeed if the observed count values are as shown in 4.8 and 4.9 below. This yields the following set of equations, comparable to those in section 3:

The observations are

$$o_1 = I_1u_1 + I_2u_2 \quad (4.1)$$
$$o_2 = I_1u_1xK + I_2u_2LK \quad (4.2)$$

The compliance condition is

$$x \geq L_o \quad (4.3)$$

The rules for establishing the values of the unknowns are

$$u_1 = CR(x)/I_1 \quad (4.4)$$
$$u_2 = C(1 - R(x))/I_2 \quad (4.5)$$

It is also known that[6]

$$u_1 > 0 \quad (4.6)$$
$$u_2 > 0 \quad (4.7)$$

Note that unless the compliance condition holds, R will not be between 0 and 1 and one of the u's in 4.4/4.5 will go negative; so 4.4/4.5 cannot be used with non-compliant values of x. If the inspected party is compliant and uses 4.4 and 4.5,

$$o_1 = C \quad (4.8)$$
$$o_2 = CKL_o \quad (4.9)$$

Clearly these observed values do not reveal any information about the value of x. One the other hand, just from equations 4.1 and 4.2 we see that, if the compliance condition is *not* fulfilled and $x < L_o$

$$\begin{aligned} o_2 &= I_1u_1xK + I_2u_2LK \\ &< I_1u_1LoK + I_2u_2LK \\ &= I_1u_1L\,K + I_2u_2LK + I_1u_1\,(Lo - L) \\ &< I_1u_1L\,K + I_2u_2LK \\ &= LKo_1 \\ &< LoKo_1 \end{aligned}$$

This means that 4.8 and 4.9 *cannot* be satisfied, so the process must fail.

5. Solving the Basic Verification Problem

The examples above suggest that although some types of verification problems may be amenable to this approach, others may not.

The question is: given a model of a set of measurements (e.g., 3.1, 3.2, 3.3) how can one compute the values of the unknowns (the functions *u,* e.g., 3.4, 3.5), and when will this process provide a system that will satisfy the conditions in section 2?

A general, abstract theorem on the existence of a solution is provided in the appendix, but for practical situations the following process should suffice. Note that according to the first condition in section 2, the observed values cannot depend on the sensitive value; this means the functions for computing the unknowns must basically invert the observation functions. For example, from section 3:

$$o_1 = x + u_2(x) \quad (3.1)$$
$$o_2 = u_1 + u_2(x) \quad (3.2)$$

can be solved to give, since the *o's* are *fixed* unknowns:

$$o_1 - x = u_2(x)$$
$$o_2 - o_1 + x = u_1(x)$$

This process provides the form of the functions *u* up to unknown constants *o*. One must then see if values of these constants can be found that allow one to satisfy the compliance conditions. In this case, the fact that the *u's* must be positive gives immediately $o_1 > x > o_1 - o_2$, and it is clear what the *o's* must be from looking at the compliance condition 3.3; and the problem is solved (and the solution is, of course, the equations 3.4 and 3.5).

It is also clear that unless one allows o_1 to be infinite, this model of observations is inconsistent with a compliance condition of the form $x > L$; this verification problem has no solution. Some experimentation also suggests that straightforward, simple, realistic measurement models will not allow one to verify complex compliance conditions, involving, for example, disconnected sets (e.g., x equals either A or B). Extending the approach to address this limitation is the subject of the next section.

6. Enhanced Procedure

This approach will require we loosen somewhat the requirements of section 2 to allow for a probabilistic approach. The new requirements will be:

(1) Any conforming value of the sensitive parameter must yield the same *probability distribution* of observed values as any other conforming value; in this case the procedure should succeed with probability one.
(2) If the sensitive value does not conform the compliance condition, the procedure must fail with some fixed probability greater than zero.

The fact that we don't specify some high detection probability should not be troubling, since, because there is zero false alarm probability and no information loss, the procedure can be repeated as often as needed to raise the detection probability to any desired level.

The idea of the enhanced procedure is that the inspectee will declare that certain results will occur if the inspector makes certain measurements. It is clear that if these statements are true, the compliance condition will be satisfied; the declarations logically imply compliance. The inspector is allowed to choose among some subsets of these statements to verify. The fact that any statement could be verified guarantees some detection probability; the *subsets* have to be structured to protect sensitive information.

Example 1

The compliance condition is $x = A$ or $x = B$ for some weight x. Some L greater than A or B is chosen and two weights are prepared, $u_1 = L - A$ and $u_2 = L - B$. The inspectee declares that these are the values of the weights, without revealing which is which. The inspector is shown the two unknown weights and is given the choice of (1) weighing x with one of the unknown weights u chosen by the inspectee (the result of which will be L); or (2) measuring the two unknown weights individually, but not measuring x. Clearly the statements

$$u = u_1 \text{ OR } u_2$$
$$x + u = L$$

$$u_1 = L - A$$
$$u_2 = L - B$$

implies the compliance condition $x = A$ or $x = B$. If the inspectee is non-compliant, at least one of the statements must be false. The first two conditions are verified if the inspector makes choice (1), the second two if he makes choice (2). If he chooses each with probability one half, he is guaranteed at least a 50 percent detection probability. The probability distribution of the observed measurements are:

with probability 0.5, $x + u$ is observed to result in the value L

with probability 0.5 the observed weights of u_1 and u_2 are $L - A$ and $L - B$.

This probability distribution holds regardless of the actual value of x. No parameters of this probability distribution are sensitive. If the procedure is repeated n times, the probability of detection is $1 - (0.5)^n$. Clearly, if the procedure is repeated, new unknowns have to be used or their identities disguised.

Example 2

Suppose one wishes to verify that the total inventory (weight) of a number of sensitive items is a certain value, *T;* however, the items are stored in two different locations, and it is not possible to weigh them all together at one time. Nor is it considered feasible to transport 'unknown' weights from one location to the other. The total weight at each location is considered sensitive.

To simplify the example as much as possible we will consider two items with weights x and y; we wish to verify $x + y = T$. Neither the items nor unknown objects can be transported between the sites. We will assume the scale has finite accuracy and reads in grams. In what follows, all values are integers.

The solution involves two sets of unknown weights and a declaration. The two sets of weights, designated u_i and v_i, have values $u_i = v_i = i$, from $i = 0$ to T grams.[7] The unknown weights are labeled with identifiers that we will designate as a_i and b_i; these identifiers give no hint as to the value of the weight and can be thought of as unique random numbers. It is important that once an identifier is assigned to a weight, it cannot be changed.[8] The declaration is a list of $T+1$ pairs of identifiers a_i, bk such that $i + k = T$.

The procedure is that the inspector is given the declaration and will make a choice between the following options:

- He can choose to verify the unknown weights. In this case he can measure any of the unknown weights he wishes, but not the sensitive objects. In particular, he can verify that for the pairs of unknown identifiers listed on the declaration, the corresponding weights sum to *T*.

  OR

- He can choose to verify the sensitive items. In this case the inspectee declares additionally the pair of identifiers *ay* and *bx*. The inspector can verify that this pair of identifiers is on the declaration (they will be since $x + y = T$); and he is allowed to measure the combined weights of the item *x* with u_y, and *y* with v_x. Both will weigh *T*.

  The procedures confirms that

  $$x + u_y = T \quad y + v_x = T \quad u_y + v_x = T$$

From this it is clear that $x + y = T$. Regardless of the values of *x* and *y*, the probability distribution of the inspectors observations are this: with probability 0.5, he will observe a set of random identifiers that identify pairs of the unknown weights that sum to *T;* with probability 0.5, he will observe a declaration with two columns of random numbers, and observe two weightings which give the result *T*.

7. Conclusion

The paper provides mathematical models of a number of situations in which a compliance condition can be verified without revealing sensitive information in a manner where both the compliance demonstration and the protection of the information is mathematically rigorous. As for real-world application, it seems clear that the models of weighing systems should work in practice, but the paper's simplified model of a gamma spectroscopy system only suggests, but does not demonstrate, that it could work in more complex measurement situations. To go the next step would involve factoring in sample weight, geometry, background, counting time, and so on. The paper shows that the basic method does not work in all situations, and indicates how to determine when it will work. The fact that this is not the end of the story is indicated by the more complicated probabilistic protocol that may work when the first approach doesn't. Still more elaborate protocols might expand the utility of the idea further.

Appendix: Formal Mathematical Model and Basic Theorems

This section provides a uniform, general treatment of the problem. It first provides a mathematical model of the observed values as functions of the sensitive parameter and unknowns, and defines what constitutes a solution to the verification problem. A theorem indicates how to determine whether such problem has a solution.

Other Examples

Two more solvable measurement models are given below.

Aa: Demonstrating that one sensitive weight is less than another

Two weight values x_1 and x_2 are sensitive. One wants to demonstrate that for some known value of *L*, $L > x_1 > x_2$ without revealing anything more about x_1 and x_2. The procedure is to pick two unknown weights u_2 and u_1, and measure the values

$$o_1 = x_1 + u_1$$
and
$$o_2 = u_2 + x_2 + u_1$$

All values are assumed to be positive. It is not hard to see that setting the unknowns at $u_1 = L - x_1$ and $u_2 = x_1 - x_2$ provides the necessary result; in this case both observed values come out to be *L*. This gives $L = x_1 + u_1$ and $x_1 - x_2 = u_2$, which demonstrates the required inequality.

Verification Procedure

	Section 3	Section 4	Section Aa	Section Ab
		Measurement	Model	
O	$o_1, o_2 > 0$	$o_1, o_2 > 0$	$o_1, o_2 > 0$	$o_1, o_2 > 0$
T	$x > 0$	$x > 0$	$x_1, x_2 > 0$	$x > 0$
S	$L_2 > x > L_1$	$x >= Lo$	$L > x_1 > x2$	$x > L$
V	$u_1 > 0$ $u_2 > 0$	$u_1 > 0$ $u_2 > 0$	$u_1 > 0$ $u_2 > 0$	$u_1 > 0$ $u_2 > 0$
f	$f_1(x, u) = x + u_2$ $f_2(x, u) = u_1 + u_2$	$f_1 = l_1u_1 + l_2u_2$ $f_2 = l_1u_1xK+l_2u_2LK$	$f_1 = x_1 + u_1$ $f_2 = u_2+x2+u_1$	$f_1 = x_1u_1$ $f_2 = u_2 + u_1$
		Model	Solution	
g	$g_1(x) = x - L_1$ $g_2(x) = L_2 - x$	$g_1 = CR(x)/l_1$ $g_2 = C(1-R(x))/l_2$	$g_1 = L - x_1$ $g_2 = x_1 - x_2$	$g_1 = K/x$ $g_2 = K/L - K/x$
o^*	$(L_2, L_2 - L_1)$	(C, CKL_o)	(L,L)	$(K,K/L)$

Ab: An additive/multiplicative model

One wishes to demonstrate that $x > L$; the observations take the form

$$o_1 = xu_1$$

and

$$o_2 = u_2 + u_1$$

All values are assumed to be positive. In this case the solution is $u_1 = K/x$, (where K is an arbitrary constant, as in the case of the section 4) and $u_2 = K/L - K/x$. This provides the observables $o_1 = K$ and $o_2 = K/L$. In this case it is clear from the second observation that $u_2 < K/L$; then from the first equation we see that $x > L$.

Compliance Model

The general case is described by a system of observations o, which depend on sensitive parameters x, and an unknowns u. The notation is intended to convey that these variables can take values in spaces that are arbitrary; they may be thought of as vectors. Call the space of observations O. It is desired to verify that x belongs to some set of values S. We know a priori that the values of x and unknowns u belong to some sets T and V respectively. Thus the "compliance model" may be described as follows. A known equation describes the observations:

$$o = f(x,u) \qquad \text{(A.1)}$$

Where f is defined on $T \times V$ and takes values in O. It is known that

$$x \text{ is an element of } T; T \text{ contains } S \qquad \text{(A.2)}$$

$$u \text{ is an element of } V \qquad \text{(A.3)}$$

The compliance condition to be demonstrated is

$$x \text{ is an element of } S \qquad \text{(A.4)}$$

Thus a compliance model may be thought of as the consisting of the objects O, T, S, V, and f.

Definition of a Solution of a Compliance Model

A function g on S taking values in V and a point o^* in O are said to solve the compliance model [O, T, S, V, f] if

$$(1)\ f(x, g(x)) = o^* \quad \text{for all } x \text{ in } S \qquad \text{(A.5)}$$

(2) for any x not in S, there exists no value of u in V such that

$$o^* = f(x,u) \qquad \text{(A.6)}$$

The verification procedure is to make the measurements resulting in an observation o and compare it to o^*; if they are equal the procedure succeeds. The function g determines how the inspected party chooses the values of the unknowns. The first condition ensures that the inspector gains no knowledge of the sensitive values x, because for any allowed values for x, the inspector observes the same data. The second condition requires that this set of data can only be observed when the sensitive values satisfy the treaty condition. The table above presents the examples of the previous sections in the language used here.

Characterization of Solutions to the Compliance Problem

The following theorem turns the problem of finding a solution to a compliance problem into a set-theoretic computation.

Let the set of points $\Omega(o)$ in $T \times V$ be defined by $\Omega(o) = f^{-1}(o)$:

$$\Omega(o) = \{(x,u):o = f(x, u)\} \quad \text{(A.7)}$$

and define a corresponding set in T by

$$\Omega_T(o) = \{ x: (x,u) \text{ is in } \Omega(o) \text{ for some } u \text{ in } V\} \quad \text{(A.8)}$$

Theorem. A solution of the compliance problem [*O, T, S, V, f*] exists if and only if there exists some observation o^* such that $\Omega_T(o^*) = S$.

Proof of sufficiency. Assume such a vector o^* exists. For each x in $S = \Omega_T(o^*)$, define $g^*(x)$ to be any u such that (x,u) is in Ω (o^*); at least one such value must exist by construction. It is claimed that g^* and o^* are a solution to the compliance problem.

Suppose x is in S. Then x is in $\Omega_T(o^*)$, which means $(x, g^*(x))$ is in $\Omega(o^*)$. By construction of the set $\Omega(o^*)$, for we have $o^* = fi(x, g^*(x))$. This proves condition (A.5) of the definition of a solution above.

Now suppose that x is not in S, and suppose there were some u such that A.7 was true. Then by definition (A.7), (x,u) would be in $\Omega(o^*)$, and by definition (A.8), x would be in $\Omega_T(o^*)$. But this contradicts the hypothesis that $\Omega_T(o^*) = S$, since x is not in S. This proves condition A.6.

Proof of necessity. Assume there is a solution to compliance problem; call this solution o^* and g^*. They satisfy A.5 and A.6. We must show $\Omega_T(o^*) = S$. If x is in S, then $(x, g^*(x))$ is in $\Omega(o^*)$ by A.6 and A.7, and therefore x is in $\Omega_T(o^*)$. If x is not S, then there is no value of u in that satisfies A.6. Therefore there is no u such that (x,u) is in $\Omega(o^*)$, so x is not in $\Omega_T(o^*)$.

Observation. The theorem depends only on the simplest set-theoretic properties of the spaces and the functions. Any one-to-one transformation will preserve these properties. This indicates that the simple mathematical forms in the examples are not an inherent feature of models that have solutions.

This result is of course very abstract. But in a practical case of nice smooth well-defined functions, the hardest part of the problem — determining 'g' up to the unknown value of 'o' — can be arrived at by the process described in section 6. Knowing this, one can effectively search the space 'O' for whether some $\Omega_T(o)$ corresponds to the right S.

Jonathan Sanborn is currently a physical science officer at the U.S. Department of State. Previous to that he held the positions of mathematician and group leader at Brookhaven National Laboratory. He has had extensive experience with the technical aspects of nuclear material accounting, IAEA safeguards, the Plutonium Production Reactor Shutdown Agreement, the Fissile Material Cutoff Treaty, the Chemical Weapons Convention, and the U.S. Additional Protocol. Dr. Sanborn holds a Ph.D. in Applied Mathematics from SUNY Stony Brook.

End Notes

1. In the case of weights one might think that one could solve this problem more simply with a pan balance with the threshold weights on one pan and the target object on the other. However, the balance is still "observing" the classified weight in the sense that the stresses and movement of the balance are a function of the classified information and one would have to assure those could not be observed. Certainly it would be possible to design a balance that *would* reveal the sensitive information.
2. There is no reason the inspector cannot know this equation, but he does not know the actual values of the *x's* and *u's*.
3. With apologies to gamma spectroscopists, for simplicity we assume the count rate is proportional to the amount of the isotope and the count ratio will equal the isotope ratio, when in reality there are lots of constants that have to be factored in. The model here is made as simple as possible to make the math transparent, and it only gives a flavor of the real physical situation.
4. K may account for differences in geometry, for example. It is not critical to the calculation.
5. One might also consider C as a counting time necessary to allow adequate counts to build up in the channels; introducing time simply complicates the issue. Mathematically, what is happening is that the solution is not unique (any *u's* with the right ratio will suffice), and choosing C fixes a solution.
6. The attenuation values must also be less than one, but that does not seem to be necessary.
7. The fact that there might be thousands of such unknown weights should not be a concern; this problem can be overcome in this case by substituting for the weights described with another set of weights where combinations of the weights can be used to make any desired value.
8. This might be assured though a containment or surveillance technique. Note that if the procedure is to be repeated, the identifiers have to be changed.

Contact Memory Buttons and Nuclear Safeguards

Jon S. Warner, Ph.D., and Roger G. Johnston, Ph.D., CPP
Argonne National Laboratory, Argonne, Illinois USA

Abstract

Contact memory buttons (CMBs) are inventory tags, not security tags. They have little or no built-in security and a number of easy-to-exploit vulnerabilities. Using CMBs to make conclusions about nuclear theft or diversion, or for tamper detection, is thus highly questionable. There may be lessons here as well for radio frequency identification devices (RFIDs), which are being considered for use in domestic and international nuclear safeguards.

Introduction

A tag is a device, applied material, or an intrinsic property that can be used to uniquely identify an object or container. Tags have a number of potential applications, including for domestic or international nuclear safeguards. One issue that is sometimes glossed over in discussions about tags is that there are really four different kinds. They differ in whether the tag is deliberately designed to deal with counterfeiting and/or lifting. *Counterfeiting* means to make an unauthorized duplicate tag that will be confused with the original. *Lifting* means removing a tag from one object or container, and then placing it in or on another without being detected.

The four kinds of tags are: inventory tags (where neither counterfeiting nor lifting are of concern), security tags (where both are of critical concern), and anti-counterfeiting tags and tokens (where only counterfeiting matters). The primary difference between an anti-counterfeiting tag (such as used to help consumer identify authentic commercial products from knockoffs) and a token (such as might be used in an arms control agreement where it is called a buddy tag) is that the latter does not necessarily need to be physically co-located with the item or container of interest.

The central concern of this paper is that existing contact memory buttons (CMBs)[1, 2, 3] (examples shown in Figure 1) are inventory tags, not security tags.[4, 5] This means that as currently designed they do not have a credible role to play in either domestic or international nuclear safeguards—which are fundamentally security applications.[6] While CMBs for nuclear applications have been used and promoted for inventory purposes, it is plain to see that CMBs are also being thought of as a tool for detecting theft or diversion of nuclear materials—a security function. This kind of mission creep where inventory devices or systems come to be viewed as providing security is, unfortunately, very common in many different areas, not just the nuclear arena.[7] It typically leads to poor security.

Inventory vs. Security

By definition, inventory systems are designed to count and locate assets. These systems will detect innocent inventory errors by insiders, but make no significant effort to counter the deliberate actions of nefarious adversaries (whether insiders or outsiders). Security systems, on the other hand, are specifically designed to deal with nefarious adversaries and their potential surreptitious attacks. This is a very different kind of application than inventory. An inventory device or system that does little or nothing to protect itself from spoofing (as is the case with commercial CMBs, including cryptographic versions) cannot provide reliable information about theft or diversion.

In our view, part of the confusion for domestic nuclear safeguards is that nuclear MC&A (material control and accountability) superficially resembles inventory, i.e., counting and locating assets. In reality, however, MC&A is really security because it is fundamentally about detecting or preventing theft or diversion of nuclear materials.[4,6] The historical tendency to (incorrectly) consider domestic and international nuclear safeguards as fundamentally the same kind of security problem is also unhelpful.[8]

Some third-party vendors have even added CMBs to tamper-indicating seals[9, 10] ostensibly to improve security (and also to automate reading the seal's unique identification number). The problem with doing this is that a seal's unique identifier must usually be damaged, destroyed, or otherwise modified during tampering, otherwise the tampering can't be detected. CMBs are extremely robust and do not satisfy this requirement. We believe that CMBs are not, at least as currently designed, appropriate for tamper detection.

CMB Mission Creep

CMBs have been employed as part of a nuclear "material inventory process" and "automated container identification system" for inventory, logistical, efficiency, and safety purposes.[11, 12, 13] This inventory process, however, is also presented (based largely on the use of CMBs) as a technique for "continuous monitoring," "surveillance," inventory "control and accountability," "automatic detection of theft," denying "access to unauthorized personnel," and sounding of alarms with anomalous conditions.[12, 14, 15] These are security functions, not inventory functions. Moreover, in a progress report on a project designed to investigate CMB nuclear applications, the developers expressed concern about people deliberately prying the CMBs off of containers with "a pocket

knife or screwdriver."[16] This is a security issue involving a nefarious adversary attempting to deliberately spoof the system; thus, in our view, mission creep is clearly occurring with CMBs.

CMBs Basics

Contact memory buttons (CMBs) are a type of electronic tag that has been applied to many different applications, including nuclear ones.[1-3] (See Figure 1.) CMBs are small round, mini-canisters that require direct contact with a reading device in order to communicate. They typically send a unique serial number, but more advanced CMBs may transmit additional information. CMBs resemble calculator batteries in shape. Sizes vary from 5 mm to 24 mm in diameter and from 0.8 mm to 12 mm in thickness. Most consist of internal microprocessors or memory chips (or both) enclosed in some type of metal housing.

Although some CMBs are active (i.e., they use batteries) the vast majority of CMBs, including those that have been applied to nuclear applications, are passive (no batteries). Passive CMB devices derive their power from the reader during the communication process. Some CMBs are read only, while others are read/write. There are even some CMBs that have a challenge/response algorithm or encryption, and are intended (at least in principle) for secure data applications.

Figure 1. Examples of three commercial contact memory buttons, with a U.S. quarter shown alongside for scale

Currently, there are three main CMB manufacturers: Oxley (E-Tag®)1, MacSema (ButtonMemory®)[2], and Dallas Semiconductor (iButton™)[3]. Oxley offers a product line consisting of 2K to 64K of memory, rugged construction, 32 bit unique serial number, and 64 bit password. MacSema's product line consists of a memory range from 128 byte to 8 megabytes worth of storage, a unique serial number, and each device is extremely rugged.

Dallas Semiconductor, which sells the most CMBs, has a large range of products based on the iButton™ such as ID only, memory devices (1K – 64K bytes), data loggers, real time clocks, password protected buttons, challenge/response buttons, and other sensor based logging buttons. Each of the iButton™ products contains a unique serial number and is extremely rugged.

Each of the three CMB manufacturers lists copious amounts of potential inventory applications for CMBs.[1-3] One company[3] mentions access control as a possible application but none of the manufacturers appears to make any substantial claims in their literature that using their product would prevent theft, diversion, espionage, sabotage, tampering, counterfeiting, or vandalism. In other words, none of the manufacturers claim to be selling a security product!

CMBs are fairly widely used for inventory applications such as animal tracking, medical bracelets, chain of custody, property tags, utility pole identification, portable databases, waste profile storage systems, time and attendance tracking, and maintenance records. In our view, these applications are appropriate uses for CMBs as inventory tags.

CMBs are also used in access control systems as electronic keys, locks, safes, deposit boxes, and voting systems.[17] Careful thought should be given, however, to whether CMBs are an appropriate technology for these types of applications because they are not security devices and (as discussed below) have serious security vulnerabilities.

CMB Lifting

A CMB needs to be attached to the container or object of interest. Adhesives, epoxies, brazing, or fasteners are typically used for this purpose. None of these fastening methods represent much of a challenge in terms of time, skill, or cost to an adversary wishing to execute surreptitious lifting. With practice, lifting usually takes 3-15 seconds. We in the Vulnerability Assessment Team[18] at Argonne National Laboratory have extensive experience in lifting tags and tamper-indicating seals affixed using these methods (including seals that are designed to fall apart on removal).[19] We have also had little difficulty in surreptitiously removing CMBs attached to tamper-indicating seals and placing them on different authentic seals, or on counterfeit seals. CMBs are extremely robust and an attacker can often get away with using a hammer and chisel to remove the CMB without causing noticeable damage to the CMB. There are of course many more elegant removal techniques that require slightly more skill.

Once the legitimate CMB is removed from a container, an adversary can place the CMB on a different or fake container, allowing him to steal the original container without being detected (at least via the CMB).

CMB Counterfeiting

Lifting is usually the easiest attack for tags in general, but counterfeiting CMBs is not particularly challenging. A considerable amount of information is available on the Internet to help with counterfeiting, including circuit diagrams for counterfeiting at least one type of CMB.

To demonstrate counterfeiting attacks, we purchased CMB evaluation kits from each of the three CMB manufacturers. These are inexpensive and readily available to anyone. (The manufacturers want to encourage the use of CMBs by making them easy to understand and use.) Evaluation kits are handy because they typically include everything needed to rapidly evaluate and understand a product. The kits contained a sampling of each company's product line as well as a reader. In this work, we focused on the low-end, non-cryptographic CMBs currently used for nuclear applications. We offer comments on the more expensive CMBs below.

To counterfeit a CMB, the attacker needs to determine the communications protocol and command format for the CMB-to-reader and the reader-to-CMB communications. Typically if a person can mimic communications in one direction he or she can mimic the other direction as well. By "communications protocol" we mean the syntax, bandwidth, and timing of the digital signals. The "command format" concerns the meanings of the various commands, handshakes, and data checks exchanged by the CMB and the reader.

A number of information sources are available in addition to the manufacturers' evaluation kits to help in reverse engineering the communication protocols and command format. [It is not necessary to reverse engineer the actual CMB, its microprocessor (if there is one), or the reader's software.] These information sources include the manufacturers' datasheets, patents, and Web sites, as well as the eagerness of their sales engineers and technical staff to help customers and potential customers understand their product. For example, one of the CMB manufacturers makes readily available a 158-page technical description of their CMBs, including details of the communication protocol and command format. This allowed us to make a counterfeit CMB circuit inexpensively and in less than two hours, including the time to read the document.

The company cannot be criticized for publicly providing such information. Firstly, their customers' design engineers will typically only use components for which they have adequate documentation. This manufacturer is simply making their product user-friendly. Secondly, this company appears to recognize that these devices aren't security devices, so it really doesn't matter that anyone can read in detail about how they work.

Also helpful to an adversary trying to reverse engineer the CMB communications protocols is the fact that CMB design engineers will generally stick with existing, well-understood communication protocols they know and understand, rather than inventing their own. There is typically a handful or so of likely communication protocols and it isn't difficult for an adversary to distinguish among them.

The remaining two CMB manufacturers do not provide detailed datasheets. One, however, lists its patents on the company's Web site. The patents, in turn, contain detailed information on the CMB circuit design and communications protocol. For the third manufacturer, we needed to do some reverse engineering. We used an oscilloscope, computer, multi-meter, and free computer port monitoring software (available on the Internet) to determine the communications protocol and command format as explained below. These are some of the most basic tools that anyone who experiments/hacks electronic circuits, from the home hobbyist to the design engineer, would possess.

The first step in this type of reverse engineering analysis is to intercept the communications between the reader and the CMB. This can be done a number of ways; some wire can be soldered onto the reader pins, for example. Next, we watch the data output through the oscilloscope. By using the oscilloscope, it is possible to deduce the functions of each pin (for multiple-pin CMBs) and determine the communications protocol.

Once the communication protocol is discovered, it is relatively easy to determine the command format. A relatively quick method is to employ software-based serial and USB port monitors to "listen in" on the CMB and reader communications.

With both the communications protocol and the command format understood, it is a simple matter to create a circuit designed to mimic the CMB of interest. Once the initial circuit is proven to work, the circuit can be miniaturized and hidden inside a counterfeit mini-canister so that the finished product looks just like a legitimate CMB.

Some CMBs have their unique serial number etched into the face of the CMB by the manufacturer, ostensibly for security purposes. It is not difficult for an adversary to mimic the etching on a counterfeit canister. We are, however, unaware of any CMB users who actually check this etched serial number since the main point of using CMBs is to automate the reading of serial numbers. What the etching does instead is make it possible for an adversary to learn the CMB's serial number without having to make physical contact with the CMB or having to power it up. The etched serial number can be read from one meter away with the naked eye, and from a distance greater than several meters with a small hand-held telescope. Rather than enhancing security, the etching appears to decrease it because it makes counterfeiting easier for an adversary.

CMB Reader Attacks

While it is unnecessary—given the ease with which CMBs can be lifted or counterfeited—it is nevertheless possible to attack or counterfeit the reader instead. This involves, respectively, modifying the existing reader or swapping it for a fake reader with the intent in either case of making the reader (or apparent reader) respond in a way that benefits an adversary.

To attack the reader, the adversary typically needs access to the reader for ten seconds to one minute to make modifications to the software or database, or to add electronic components. The latter can include adding miniature radio frequency (rf) modules to control the behavior of the reader from a distance (and the CMB serial numbers it reports). For counterfeiting, the adversary would purchase or steal an identical reader to what is being used, modify it at his leisure in his own facility, than swap it for the original reader in the field. The latter typically takes less than three seconds for a hand-held reader.

More Advanced CMBs

More advanced CMBs (not currently used for nuclear applications) can include such features as password protection, physical or electronic tamper detection, key erasure, and/or encryption. These features often make the CMB significantly more expensive and require it to have a battery.

None of these features currently appears to offer much meaningful additional security. Simple (non-challenge/response) password protection for low-cost passive CMBs is of little value because the password is typically sent (unencrypted) from the reader to the CMB for authentication. The password can easily be intercepted by an adversary along with the rest of the communication stream. Alternately, the adversary can make a fake CMB that accepts any password and then produces the correct serial number. More complex, multiple-password CMBs have been beaten with relatively simple dictionary type attacks.[20, 21]

While we have not experimented with the electronic or physical tamper detection features on advanced CMBs in any detail, they do not appear to be either sophisticated or difficult to defeat, nor much different from tamper detection features we have previously found easy to defeat for security devices not based on CMBs. As far as encrypted CMBs are concerned, cryptoanalytic attacks and a variety of other attacks are possible,[22] but it is probably much easier just to open up the CMB canister and either bypass the encryption or read out the key. Encryption or data authentication add little security when the sending and/or receiving stations have poor physical security, as appears to be the case even for advanced CMBs and CMB readers.

Discussion

Current CMBs are inventory tags, not security tags because they lack effective means to prevent lifting or counterfeiting, or even spoofing of the reader. As inventory tags, they may well be useful for inventory purposes to provide greater efficiency and safety, and to reduce logistics errors in the handling of nuclear materials. Current CMB designs, however, do not provide effective security, and should not be used as a part of a domestic or international safeguards program to make conclusions about nuclear theft or diversion.

Now nuclear safeguards and security is traditionally based on having multiple layers of security. No security device or technology exists in isolation. Thus, the (inevitable) security vulnerabilities in any layer or technology are not necessarily catastrophic if the vulnerability is recognized, the overall security or safeguards program can be designed to compensate, and if having multiple layers of security are not used as an excuse to avoid dealing with correctable weaknesses in any given layer or technology.[2,3] The problem as we see it with CMBs is not compensating for a minor vulnerability or two, but rather that they are not fundamentally security devices. Except for a complete redesign of CMBs and their readers—building from the ground up with security in mind and employing effective tamper detection, anti-counterfeiting, and anti-lifting features—we believe it is difficult to detect or mitigate the attacks discussed in this paper. Other attacks may be possible as well.

A similar problem exists for radio frequency identification devices (RFIDs). These are increasingly being proposed for use in domestic and international nuclear safeguards. RFIDs are essentially non-contact CMBs that communicate via rf signals. As inventory tags with little or no security built in (just like CMBs), we believe RFIDs (as currently designed) are also inappropriate for nuclear security applications. We are currently preparing a paper discussing our experiences with RFID vulnerabilities.

Disclaimers and Acknowledgements

The views expressed in this paper are those of the authors and should not necessarily be ascribed to Argonne National Laboratory, Los Alamos National Laboratory, or the United States Department of Energy. Anthony Garcia, Leon Lopez, Ron Martinez, Adam Pacheco, and Sonia Trujillo contributed significantly to this work.

Jon Warner, Ph.D., is a systems engineer with the Vulnerability Assessment Team (VAT) in the Nuclear Engineering Division at Argonne National Laboratory. He was a technical staff member with the VAT at Los Alamos National Laboratory from 2002 to 2007. Warner's research interests include digital device forensic analysis, hardware and software reverse engineering, GPS spoofing and countermeasures, and developing novel security devices. He received B.S. degrees in physics and business management at Southern Oregon University (1994), and M.S. and Ph.D. degrees in physics from Portland State University in 1998 and 2002.

Roger G. Johnston, Ph.D., CPP, is a senior systems engineer and section manager for the Vulnerability Assessment Team (VAT) in the Nuclear Engineering Division at Argonne National Laboratory. He was founder and head of the VAT at Los Alamos National Laboratory (LANL) from 1992 to 2007. Johnston has provided consulting, vulnerability assessments, and security solutions for more than thirty government agencies and private companies. He graduated from Carleton College (1977), and received M.S. and Ph.D. degrees in physics from the University of Colorado (1983). He has authored

more than 110 technical papers and sixty invited talks, and holds ten U.S. patents. He has won numerous awards, including the 2004 LANL Fellows Prize for Outstanding Research.

References

1. Oxley E-tag homepage, http://www.oxley.co.uk/etag/
2. MacSema ButtonMemory homepage, http://www.macsema.com/ and http://www.sys-tec.com/documents/ButtonMemory%20Catalog.pdf
3. iButton: Touch the Future homepage, http://www.maximic.com/products/ibutton/ and iButton Solutions Search webpage, http://www.maximic.com/products/ibutton/solutions/search.cfm
4. Johnston, R. G., J. S. Warner, A. R. E. Garcia, R. K. Martinez, L. N. Lopez, A. N. Pacheco, S. J. Trujillo, A. M. Herrera, and E. G. Bitzer. 2005. Nuclear Safeguards and Security: We Can Do Better, 10th International Conference on Environmental Remediation and Radioactive Waste Management (ICEM'05), Glasgow, Scotland.
5. Johnston, R. G., J. S. Warner. 2005. The Dr. Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure, *Security Management* 49, 112-121.
6. Bremer Maerli, M. and R. G. Johnston. 2002. Safeguarding This and Verifying That: Fuzzy Concepts, Confusing Terminology, and Their Detrimental Effects on Nuclear Husbandry, *Nonproliferation Review* 9, 54-82, cns.miis.edu/pubs/npr/vol09/91/91maerli.pdf.
7. DeGaspari, J. 2005. Ports Look Outward, *Mechanical Engineering,* http://www.memagazine.org/contents/current/features/portslook/portslook.html.
8. Johnston, R. G., and M. Bremer Maerli. 2003. International vs. Domestic Nuclear Safeguards: The Need for Clarity in the Debate Over Effectiveness, *Disarmament Diplomacy* 69, 1-6, http://www.acronym.org.uk/dd/dd69/69op01.htm.
9. Rubanenko, N., J. Griggs, J. Smoot, J. and Tanner. 2000. Tags and Seals in a Transparency Regime, Pacific Northwest National Laboratory Report PNNL-SA-33342, http://amtl.iwapps.com/pdfs/2000/00000180.pdf.
10. CGM Security, Button Memory Technology, http://www.cgmsecuritysolutions.com/sw/swchannel/productcatalogcf_v2/internet/model.asp/ProductMasterID/20048/ParentID/22174/SWSESSIONID/peazrzcrlszhll.
11. Pickett, C. A. 1999. Active Tag and Seal Technologies Designed for the Unattended Monitoring of Stored Nuclear Materials, *Proceedings of the Fourth Security Seals Symposium,* 69-74.
12. Rumyantsev, A. N., V. A. Pavshuk, L. Y. Tikhonov, Z. W. Bell, R. L. Lawson, L. R. Mooney, C. A. Pickett, J. R. Younkin, and S. P. Singh. 1999. Automated Systems for Unattended Weight and Item Monitoring at the Kurchatov Institute in Moscow, Russia, http://nnp.ornl.gov/orsens/pubs/inmm99_report-r.pdf.
13. Best Manufacturing Practice Center of Excellence. 1996. Best Manufacturing Processes: Report of Survey Conducted at Department of Energy, Oak Ridge Office, http://www.p2pays.org/ref/05/04944.pdf.
14. Oak Ridge National Laboratory, Precision Inventory Control and Accountability: SmartShelf™ Technology, http://nnp.ornl.gov/orsens/smrtshlf.shtml.
15. Bell, Z. W., C. A. Pickett, S. F. Razinkov, A. F. Shapovalov, G. M. Skripka, and S. P. Singh. 1998. Implementation of Continuous Inventory Technologies at the All-Russian Scientific Research, http://nnp.ornl.gov/orsens/pubs/INMM98.pdf.
16. Bell, Z. W., R. L. Lawson, and C. D. Long. 1996. SmartShelf™ Report of Activities for Fiscal Year 1996, Y12 Plant Report Y/DW-1645, http://www.osti.gov/bridge/product.biblio.jsp?osti_id=446377&query_id=0.
17. See, for example, Be-Tech Web site, http://www.be-tech.com.hk/2083-2212B.htm; TimePilot Web site, http://www.accesspilot.com/; iButton Web page, http://www. maximic.com/products/ibutton/solutions/search.cfm? Action=DD&id=177; Creative Control Concepts, iButton Digital Key Access System for Home Automation & Security Systems, http://www.cc-concepts.com/products/ilock/ilock.pdf; Pennsylvania Voting Task Force, Task Force Recommendations, March 2001, 41, http://www.dos.state.pa.us/bcel/ lib/bcel/pdf/tfreportfinal.pdf; Clausen, D., Puryear, D., Rodriguez, A., "Secure Voting Using Disconnected, Distributed Polling Devices", June 5, 2000, http://www.dclausen.net/projects/voting/cs444n_voting_report.pdf; and VoteHerePlatinum, Vote Here Election System, Version 2.2 Platinum, Voters User Guide, http://www.riik.ee/evalimised/tehnoloogia/usermanual.pdf.
18. Vulnerability Assessment Team. 2008. http://www.ne.anl.gov/capabilities/vat.
19. Johnston, R. G. 2006. Tamper-Indicating Seals, *American Scientist 9*4, 515-523.
20. Grand, J. 2004. A Historical Look at Hardware Token Compromises, http://www.blackhat.com/presentations/bhusa-04/bh-us-04grand/grand_hardware_token_US04_handouts.pdf.
21. Grand, J. 2001. Security Advisory, http://www.grandideastudio.com/files/security/tokens/ds1991_ibutton_advisory.txt.
22. Anderson, R., and M. Kuhn. 1996. Tamper Resistance—A Cautionary Note, http://www.usenix.org/publications/library/proceedings/ec96/full_papers/kuhn/index.html.
23. Johnston, R. G., J. S. Warner, and E. G. Bitzer. 2007. How to Design a Physical Security Device, System, or Program, *Proceedings of the American Society for Industrial Security Annual Meeting.*

Hypothesis Testing: Frequentist Versus Bayesian With Examples from Nuclear Safeguards

Tom Burr, Los Alamos National Laboratory, Los Alamos, New Mexico USA
Dennis Weier, Pacific Northwest National Laboratory, Richland, Washington USA

Abstract

Bayesian data analysis continues to gain popularity, largely due to effective adaptation of Markov Chain Monte Carlo for the purpose of numerically investigating features of the posterior probabilities of interest. In nuclear safeguards, Bayesian approaches are occasionally advocated. This paper provides a simple explanation of the Bayesian approach, illustrates its possible use on example nuclear safeguards analyses, and discusses the controversy surrounding its use on other nuclear safeguards analyses.

1.0 Introduction

Thomas Bayes introduced Bayes rule more than 200 years ago (Gelman et. al., 1995). The rule has never been controversial, but application of the rule remains controversial in particular settings. One such setting is the testing of a simple hypothesis, which we examine in this paper.

Examples of hypothesis testing in the context of safeguards at a facility under safeguards include: (1) monitor a facility and periodically check for evidence that nuclear material has been diverted, and (2) randomly select items for verification measurements and check for evidence of material diversion from these items. In the context of U.S. border security, another example is to monitor vehicle traffic at borders and test each vehicle for evidence against the hypothesis that it contains no illicit special nuclear material (SNM).

Some ("Bayesians") believe that examples such as the above are best treated in a Bayesian framework, in which the posterior probability describes our belief that material has been diverted from the facility, or from particular selected items. Others ("frequentists") believe it is better to calculate the probability of observing anomalous data assuming either that there has been no diversion (false alarm rate), or assuming that there has been diversion of a specified amount or larger (detection probability).

The essential difference between Bayesians and frequentists is as follows. Bayesians treat each parameter (such as the true amount of missing SNM) as a random variable having a probability distribution before observing any data (the "prior distribution"), and after observing data (the "posterior distribution"). Suppose the parameter T of interest is the true amount of missing SNM. Then the mean and standard deviation of the posterior distribution of the random variable T provide an estimate of the true amount of missing SNM, and the uncertainty in the estimate is characterized by the standard deviation. Frequentists regard T as an unknown to be estimated using statistics calculated from data. Although these approaches sound similar, distinctions between Bayesian and frequentist approaches continue to be a research area.

2.0 Bayes Rule

Let S denote the sample space of an experiment. Let $A_1, A_2, \ldots, A_k$ be k events in S such that any pair A_i, A_j for $i \neq j$ are disjoint (have empty intersection), and $\cup_{i=1}^{k} A_i = S$. Then the events $A_1, A_2, \ldots, A_k$ are said to form a partition of S. Let B be any event in the sample space S with $P(B) > 0$. Let $P(A_i|B)$ denote the conditional probability that event A_i occurs given that event B occurs, defined as $P(A_i|B) = P(A_i B)/P(B)$. Then Bayes rule is:

$$P(A_i|B) = \frac{P(B|A_i)P(A_i)}{\sum_{j=1}^{k} P(B|A_j)P(A_j)} \quad (1).$$

Bayes rule follows easily from the definition of conditional probability and can be informally visualized using a Venn diagram where the events A and B intersect. Suppose we know the conditional probability $P(B|A)$. Then what is the probability $P(A|B)$? The need for Bayes rule arose from the fact that we are often given, but we want to calculate $P(A|B)$. Bayes rule, Equation 1, is a trivial extension from the two-event (events A and B) partition of S. In a common setting, the *likelihood* of the data x assuming hypothesis A is given by $P(x|A)$ and we apply Eq. (1) to compute $P(A|x)$, the probability of hypothesis A given the data x.

In all the examples below, the posterior probabilities such as $P(A|x)$ can be computed analytically, without resorting to numerical integration. Burr et al. (2005) provide a recent nonproliferation example where numerical integration via Markov Chain Monte Carlo (MCMC) is compelling. Beginning in the mid-1990s, MCMC has made Bayesian analyses more effective, largely by allowing users to choose realistic prior probabilities and/or probability models for the data without much concern regarding whether they are analytically convenient.

3.0 Examples from Nuclear Safeguards

3.1. Inventory Difference Evaluation

Example 1 will illustrate the terminology, and illustrate testing a simple hypothesis. The example is a common one involving monitoring declared nuclear facilities.

Suppose that every month a facility that processes SNM must measure its inventory and estimate the amount of missing material in a quantity called the inventory difference (ID). Due to measurement error, the measured ID will vary randomly around ID_{true}, with a distribution that is well approximated by a normal distribution with mean IDtrue, and standard deviation σ_{ID}. By convention, if there is a material loss then $ID_{true} > 0$, and if there is a material gain, then $ID_{true} < 0$.

Observe the facility ID for one inventory period. One way to partition the sample space is:

$A_1 = \{ID_{true} = 0, ID \geq 2\ \sigma_{ID}\}$, $A_2 = \{ID_{true} = 0, ID < 2\ \sigma_{ID}\}$,

$A_3 = \{ID_{true} > 0, ID \geq 2\ \sigma_{ID}\}$, $A_4 = \{ID_{true} > 0, ID < 2\ \sigma_{ID}\}$, and $A_5 = \{ID_{true} < 0\}$.

To limit the discussion, we ignore the possibility that $ID_{true} < 0$, so we assume that $P(A_5) = 0$. However, as an aside, a diverter's strategy involving removing and replacing material could be effective as a means of increasing the variation in observed *ID* sequences. If we assign $P(A_5) = 0$, then $\{A_1, A_2, A_3, A_4\}$ form a partition of the sample space, and so Bayes rule will apply.

Suppose we observe a large ID, say $ID = 2\sigma_{ID}$. We want to test the simple hypothesis: H_0: $ID_{true} = 0$ versus the alternative hypothesis H_A: $ID_{true} > 0$. The frequentist test proceeds as: assume H_0: $ID_{true} = 0$ is true; calculate a test statistic, *S*, and if $P(S > S_{observed} \mid H_0$: $ID_{true} = 0$ is true) $\leq .05$, then "reject" H0 at the significance level 0.05.

Let *Z* denote a random variable having a normal distribution with mean 0 and variance σ^2. Then $P(Z > 2\sigma) = 0.025$. Therefore, the test of H_0 is "rejected at the .05 significance level" because the test statistic $S = \frac{ID}{\sigma_{ID}}$ and $P(S > 2) = 0.025 \leq 0.05$, and for the test of H_0: $ID_{true} = 0$, the so-called "p-value" is 0.025 corresponding to the event $ID = 2\sigma_{ID}$. Qualitatively, the conclusion is: "if H_0 is true then the data is very unusual, so we prefer to believe that H_0 is not true." But what if we ask: "what is the probability that H_0 is false?" Answer: We lack sufficient information to answer. Here is why. We seek the conditional probability $P(H_0$ is false $\mid ID \geq 2\sigma_{ID})$. Let *D* denote the event "diversion attempted," and *A* denote the event "anomaly indicated" (for example, *A* could be the event $ID \geq 2\ \sigma_{ID}$). Then by straightforward application of Baye's rule

$$P(D|A) = 1/(1+(1-\pi)\alpha\ /(\pi\ (1-\beta)), \qquad (2)$$

where π is the *prior* probability of attempted diversion, $\pi = P(D)$, β is the false negative probability, and α is the false positive probability (Speed and Culpin, 1986). The false positive probability $\alpha = P(ID \geq 2\sigma_{ID} \mid H_0$ is true) = 0.025 in this example.

Concerning the unknowns, we don't know the probability that $\pi = P(D) = P(H_0$ is false) and see no defensible way to estimate it . And, $\beta = P(ID \geq 2\sigma_{ID} \mid H_0$ is false) depends on the particular value of ID_{true}. Consider two extreme cases: $ID_{true} \cong 0$, and $ID_{true} = 3\sigma_{ID}$. If $ID_{true} \cong 0$, then $P(ID \geq 2\sigma_{ID} \mid H_0$ is false) $\cong 0.025$. If $ID_{true} = 3\sigma_{ID}$, then $P(ID \geq 2\sigma_{ID} \mid H_0$ is false) $\cong 0.84$. So, we cannot answer the question by applying Bayes rule unless we know both of our unknowns.

We will illustrate that different conclusions would be reached depending on values assigned to the two unknowns. We record the desired conditional probability, $P(H_0$ is false $\mid ID\ 2\sigma_{ID})$ for six cases in Table 1. To be specific, we replaced $ID_{true} \cong 0$ with $ID_{true} = 0.001\ \sigma_{ID}$.

Table 1. Cell entries are $P(D|A) = P(H_0$ is false $\mid ID \geq 2\sigma_{ID})$ for six cases, determined by the prior value $P(H_0$ is false) and the value of ID_{true}

	$\pi = P(D) = P(H_0$ is false)		
ID_{true}	0.99	0.5	0.01
$ID_{true} = 0.001\ \sigma_{ID}$ $\beta = 1 - 0.025 = 0.975$	0.99	0.5	0.01
$ID_{true} = 3\ \sigma_{ID}$ $\beta = 1 - 0.84 = 0.16$	0.9997	0.97	0.25

We see in Table 1, that $P(H_0$ is false $\mid ID \geq 2\sigma_{ID})$ varies from nearly 0 to nearly 1 depending on the two unknowns. If the alternate hypothesis is H_A: $ID_{true} = 0.001\ \sigma_{ID}$, then we would not expect the data to be able to distinguish between H_0 and H_A. That is what we observe in Table 1, because the prior probabilities, $P(H_0$ is false), which are equal to 0 .99, 0.5, and 0.01, are not changed by observing $ID \geq 2\sigma_{ID}$. If the alternate hypothesis is, $ID_{true} = 3\sigma_{ID}$ then we would expect our data to distinguish between H_0 and H_A. But what will happen if the data contradict the prior? If $ID \geq 2\sigma_{ID}$ but $P(H_0$ is false) = 0.01, we say that the data ?contradict the prior.? In the case shown in the (row 3, column 3) entry in Table 1, the data has ?updated our prior? to the posterior

$P(H_0$ is false $\mid ID \geq 2\sigma_{ID}) = 0.25$. If the data "support the prior" (row 2, column 1) then the posterior $P(H_0$ is false $\mid ID \geq 2\sigma_{ID}) = 0.9997$. And if the data "neither support nor contradict the prior" (row 2, column 2) then the posterior $P(H_0$ is false $\mid ID \geq 2\sigma_{ID}) = 0.97$, so $P(H_0$ is false $\mid ID \geq 2\sigma_{ID}) = 0.03$, which is close to the frequentists' "p-value" of 0.025.

Caution is always given that the frequentists' "p-value" of 0.025 cannot be interpreted as the probability $P(H_0$ is true $\mid ID \geq$

$2\sigma_{ID}$). Table 1 provides one example why not; such a conditional probability depends on unknowns that the frequentist might regard as unknowable.

Equation 2 implies that if π is small, then most alarms will be false. For example, see the two column-3 entries in Table 1, for which $\pi = 0.01$, are $P(D|A) = 0.01$, or 0.25, so 99 percent or 75 percent of alarms are false, depending on the value of β. For various reasons, many safeguards practitioners believe that π is small for monitored facilities, provided that effective safeguards is maintained.

Bayesian Decision Theory

Bayesian decision theory uses Bayes rule to compute the expected cost of misclassification. Having to specify the prior and sensitivity of conclusions to misspecifying the prior is one objection to a Bayesian analysis. However, the Bayesian view is that the Bayesian expected misclassification cost (EMC), involving the probability of false alarm or of failure to detect diversion, and the *costs* of those two undesired events, is, or should be, the logic behind any procedure. This means that so-called non-Bayesians (frequentists) sometimes operate as Bayesians, but with hidden assumptions about priors and costs. For example, let f = false alarm cost, and d = undetected diversion cost, then the expected cost is

$$E(Cost) = d\pi\beta + f(1-\pi)\alpha. \quad (3)$$

Assuming that at least subconsciously, we seek to minimize E(Cost), Bayesians argue that Equation 3 forces us to realize that when we *arbitrarily* opt for specific small values of α and β, we are implicitly assuming something about the relative values of π, d, and f.

However, because there need not be any attempt to separately specify π (diversion probability) and d (undetected diversion cost) in the expected cost given by Eq. (3), the frequentist does not claim to be attempting to minimize E(Cost) when selecting values for α and β. Instead, a frequentist might choose α and β on the basis of the cost f of false alarms, or perhaps by choosing a decision threshold and corresponding α and β on the basis of where the estimated relation between β and α suggests a good choice. For example, if β could be substantially reduced for a relatively small increase in α, it would be defensible to lower the threshold and accept the small increase in α. In addition, it is typical to define a significant quantify (SQ) of SNM such that a safeguards goal is to have small β (0.05 for example) if the true SNM loss is one SQ or more while maintaining a small α (0.05 for example) It is then possible to evaluate whether the σ_{ID} for candidate assay methods will be sufficiently small to meet these goals. This provides an objective safeguards effectiveness measure that avoids separate specification of d and π.

3.2 Verification Measurements

A Bayesian approach to sampling was presented by Gorbatenko et. al. (2006) in which the true defect probability p_D (an unknown parameter) among N stored items was regarded as a random variable. A defective item could be defined as one that is missing any amount of material, or perhaps as missing more than some threshold amount of material.

Because the choice of prior probability for p_D is controversial in this context, many safeguards specialists prefer a frequentist approach to sampling. In the typical frequentist approach in safeguards, a sample size n is calculated that guarantees a large probability, say 0.95, that at least one defect will be detected in the sample if p_D exceeds some value, such as 0.01. This is somewhat of a "statistical sleight of hand" because the desired defect rate is usually $p_D = 0$ (depending on the amount of SNM per item) but the sample size required to test $p_D = 0$ versus $p_D \geq 1/N$ is prohibitively large. For example, to have 95 percent detection probability requires that the sample size n is 95 percent of the population size N.

Smaller sample sizes can be recommended if instead the probability of observing at least one sample defect (and thus "failing the inspection") when $p_D \geq 0.01$ is calculated as a function of sample size. Very similar sample sizes arise via similar calculations if the goal is to conclude with probability no less than 0.95 that $p_D < 0.01$. For example, in a population of $N = 10{,}000$ items, a sample of size of 289 using zero-defect sampling will reach this goal. This is a sample size of only 2.9 percent of the population size. All these calculations use the well-known hypergeometric distribution that determines probabilities of various numbers of sample defects as a function of sample size, population size, and p_D. Again, this is somewhat of a "statistical sleight of hand" for the purpose of achieving small sample sizes, because the real goal is typically to conclude with high confidence that $p_D = 0$, unless each item has much less than a significant quantify of SNM.

Gorbatenko et. al. (2006) assumed a uniform prior for p_D on [0,1] to reflect maximal ignorance prior to sampling. However, even this *noninformative* prior will impact some analyses, causing, for example, point estimates of p_D to be closer to 0.5 (the mean of the prior) than are frequentist point estimates of p_D. Furthermore, a uniform prior for p_D conveys different information, about, say p^2_D, or other transformations of p_D. Clearly, Bayesian approaches can be controversial, mostly arising from choice of the prior and interpretations of subjective probabilities.

After making verification measurements on each of n items, a frequentist would probably perform either a hypothesis test of H_0: $p_D = 0$ versus H_1: $p_D \geq 0.01$, or construct a confidence interval for p_D. The analogous Bayesian concepts are the posterior probability that $p_D = 0$ and the posterior predictive interval for p_D. However, in order to calculate the probability that $p_D < 0.01$, it is necessary to regard p_D as a random variable and assign a prior probability to $P(p_D < 0.01)$. A frequentist refuses to do this, perhaps causing frustration. A Bayesian does not hesitate to calculate $P(p_D < 0.01)$, but is obliged to assess sensitivity to the prior.

Gorbatenko et. al. (2006) showed that if a uniform prior is assumed for p_D, then the required frequentist sample size in the hypothesis testing setting using H_0: $p_D = 0$ versus H_1: $p_D \geq 0.01$ is the same as the required Bayesian sample size for the $P(p_D < 0.01)$ formulation of the problem. The same can be shown for the confidence interval approach versus the posterior predictive probability approach. Therefore, in this case, there is no practical difference whether one adopts a Bayesian or a frequentist view. However, the interpretations are considerably different.

The "similar sample size result" in Gorbatenko et. al. (2006) is not unusual. Very often, the Bayesian analysis using the "maximum entropy" or a "noninformative" prior gives the same or very nearly the same results as the frequentist approach (Gelman et. al., 1995). However, most Bayesians would agree in the safeguards context that even if p_D is thought to be near zero because no defects have been observed in previous samples, it is inappropriate to include such information in the prior. This is because past history is irrelevant in this case. Contrast this reluctance to use past history with the medical example below, where past history is the prevalence of breast cancer in the general population, which certainly is useful information.

In either the Bayesian or frequentist approach, the number of sampled defects required to fail the inspection depends on details of the sampling plan that need not concern us here. And again, the required sample size to make the same quality of inference statement (95 percent or 99 percent confident that $p_D < 0.01$ for example) is essentially the same for the frequentist and Bayesian approach if a uniform prior is chosen in the Bayesian approach.

In both cases, we cannot achieve what we would like, which is high confidence that $p_D = 0$. Therefore, we either settle for making confidence statements that $p_D < 0.01$ for example, or we invoke a nonuniform prior for p_D, arguing that few or no defects have ever been detected so there is high probability that $p_D < 0.01$ prior to collecting more data. The former choice remains in effect for the audit-type activities associated with safeguards-related verification measurements because the "trust but verify" view seems to be the most appropriate.

3.2.1 Bayesian Decision Theory

Again suppose that n items will be inspected in a storage facility having N sealed items, each containing at least 1 SQ of SNM so that it is important to ensure that 100 percent of the N items are intact. How large should n be? Assume the time to inspect each item is t hours, then the detection probability is $n/N = T/(Nt)$ assuming a total effort of T hours. Assume the adversary will gain advantage d for undetected illegal behavior (diversion), advantage 0 for legal behavior, and lose advantage b for detected illegal behavior. Then the adversary's expected advantage *(utility)* if he behaves illegally is $U = d(1-n/N) - bn/N$ and if $U < 0$, then the adversary will be inclined toward legal behavior.

We could then choose $T > Nt/(1 + b/d)$ to strongly discourage illegal behavior, which implies that for large b/d values, a small effort T is suitable for deterrence (Avenhaus and Canty, 1999). There is an assumed positive payoff to the adversary for undetected diversion, negative payoff for detected diversion, and zero payoff for legal behavior. Similar payoffs exist for the inspector. In this case, it has been shown that we need either a strong penalty for detected diversion or very high detection probability. This is shown via an effective and simple cost/benefit argument in (Avenhaus and Canty, 1999).

In Avenhaus and Canty (1999), regarding how much inspection effort is appropriate at a declared facility, the authors state, "The obvious and only answer is that the inspector should invest that amount of verification effort which will deter the facility operator, through the risk of timely detection, from illegally breaking a seal, no more and no less." This statement helps emphasize two issues: First, Bayesian decision theory literature (Speed and Culpin, 1986; Avenhaus and Canty, 1999) has considered only those hypothetical states under safeguards that seek to divert material. Many *adversaries* under safeguards instead want to cooperate fully to prove that safeguards is effective and that they are compliant. Therefore, the notion of inspecting to provide a deterrent is irrelevant. Second, even the rare facility that is a true adversary will have unknown or difficult-to-quantify cost/benefit values, as will the inspector. Therefore, the appropriate amount of inspection effort (in terms of false positive and negative rates) is typically thought to be a subjective, ad hoc, but reasonable choice. However, once the false positive and negative rates are chosen, this does imply that the expected cost is minimized only for a certain choice of cost/benefit values. This implies that any frequentist approach is optimal in a Bayesian context only for a particular unconscious choice of cost/benefit values.

3.3 Constrained Regression

A Bayesian approach to estimate and test hypotheses related to the radiation signature at U.S. borders in vehicle profiles (time series of gamma counts) is presented in Gattiker and Burr (2006). In this example, the goal is to detect illicit nuclear cargo. In the setting of interest, the background count rate, the profile length, and the background suppression due to the vehicle each vary from vehicle to vehicle. The parameters to be estimated for each vehicle profile are the coefficients for a basis decomposition, and the Bayesian approach is useful because it provides uncertainty estimates and it can impose nonnegativity constraints on these parameters. Such constraints are easily captured by choice of the prior distribution simply by choosing a prior distribution that puts zero probability on negative values.

Of course no constraint is valid if it arises from bad assumptions. But constrained parameter estimation is established as an effective approach because parameters are often nonnegative by definition. In that case, the Bayesian view provides the proper foundation and MCMC or analytical alternatives provide a practical implementation. Closed form analytical approaches such as penalized likelihood can be effective, and are often implemented

in a frequentist framework. However, the Bayesian view justifies the particular penalty choice and therefore provides the proper foundation (Gelman et. al., 1995). In some cases, the Bayesian view also simplifies implementation.

Generally, the sometimes-subjective choices for the prior probabilities for the parameters are the reason for much of the controversy. And, these prior probabilities oblige the Bayesian to perform sensitivity-to-the-prior studies, which can be quite time consuming. However, in cases such as this example of constrained regression, which involved choosing a prior allowing only non-negative values, the prior probability is less controversial. Furthermore, the Bayesian approach is the among the simplest options for including confidence statements regarding parameters that are constrained to be nonnegative.

3.4 Lower Limit of Detection

There are many safeguards applications for the concept of a lower limit of detection (LLD), including environmental sampling applications and stand-off verification measurements. Lloyd (1968) is a key reference, and it uses a frequentist approach. The main challenge is to estimate the likelihood for the background and for the background plus signal. The frequentist approach specifies the smallest signal that can be detected at a given false negative rate for a given false alarm rate, and seems to be the most natural framework for expressing LLD concepts.

4. 0 Medical Example

Suppose that women are screened for breast cancer. The screening test has a false positive probability denoted p_{FP} and a false negative probability denoted p_{FN}. The Bayesian approach is a good choice in this example, largely because the prior probability of breast cancer can be estimated from the population.

Denote the two classes of women by $y = D$ for those having breast cancer and $y = ND$ for those not having breast cancer. We ignore "shades of gray" involving a pre-cancerous class, and seek the conditional probability P($y = D$|test is positive). The knowns regarding the diagnostic test are P(test is positive|$y = ND$) = p_{FP} and P(test is positive|$y = D$) = 1- p_{FN}. The unknown is P($y = D$).

The frequentist approach is to assume H_0: $y = ND$ and calculate the probability of observing a positive test. Because P(test is positive|$y = ND$) = p_{FP}, the "false alarm" rate is p_{FP} and the procedure will be to label all women having a positive test result as $y = D$.

The Bayesian approach is to apply Bayes rule,

P($y = D$|test is positive) = P(test is positive|$y = D$)P($y = D$)/ P(test is positive), where

P(test is positive) = p_{FP} P($y = ND$) + (1- p_{FN}) P($y = D$). Therefore, we need to know the fraction of women in the population who have breast cancer. Let p_{FP} = 0.01, p_{FN} = 0.01, and do two cases.

1) Region A with P($y = D$) = 0.5.

P($y = D$|test is positive) = (0.99 x 0.5)/(0.99 x 0 .5 + 0.01 x 0.5) = 0.99

P($y = D$|test is negative) = (0.01 x 0.5)/(0.01 x 0.5 + 0.99 x 0.5) = 0.01

Note that these two results agree with the vague notion that many people will (incorrectly) have about the "posterior" probabilities of interest.

2) Region B with P($y = D$) = 0.01.

P($y = D$|test is positive) = 0.5 and P($y = D$|test is negative) = 0.0001.

Note that these two results disagree with the vague notion that many people will (incorrectly) have about the *posterior* probabilities of interest.

4.1 Bayesian Decision Theory

A complete Bayesian analysis assigns costs to the two types of errors (a false positive decision and a false negative decision), and then uses a decision procedure that minimizes the expected Bayes cost. That would be a reasonable procedure provided we could agree on the costs of the two types of errors.

Suppose the cost of labeling a $y = D$ case as a $y = ND$ case is $C_{ND|D}$ and the cost of labeling a $y = ND$ case as a $y = D$ case is $C_{D|ND}$. Denote the decision to label a case as $y = D$ by $D(x) = D$, and the decision to label a case as $y = ND$ by $D(x) = ND$. Here, $D(x)$ represents the decision as a function of the test result x (positive or negative). Then the expected misclassification cost, EMC, satisfies EMC = $C_{ND|D}$ P($y = D$, $D(x) = ND$) + $C_{D|ND}$ P($y = ND$, $D(x) = D$). It is then simple to show that the following rule minimizes the EMC.

$D_B(x) = D$ if P($y = D|x$)/P($y = ND|x$)} ≥ $C_{D|ND}$ / $C_{ND|D}$ (4).

ND otherwise

We have used the notation $D_B(x)$ to denote that it is the Bayes rule; i.e., it is the rule that minimizes the EMC. Consider three extreme cases: (1) $C_{D|ND}$ = 50 $C_{ND|D}$, (2) $C_{D|ND}$ = $C_{ND|D}$, and (3) $C_{D|ND}$ = 0.02 $C_{ND|D}$. For case 1, the trauma of a "false alarm" is considered more costly than a "failure to detect." For case 2, the two types of errors are equal, and for case 3, the "failure to detect" causes more damage than a "false alarm." Most likely, Case 3 would be in effect, but at issue would be the actual ratio of the two costs, which we have set to fifty for this example. Frequentists might object to the *need* to assign costs to the two types of error. However, in this example, regardless of whether we explicitly set the costs, assumed costs are in effect because whatever decision criteria is used will minimize the EMC for only one particular

ratio of the two costs.

We will complete this example for region A and B for each of the 3 costs for $p_{FP} = p_{FN} = 0.01$.

For region A with $P(y = D) = 0.5$, in Case 1 with $C_{D|ND} = 50\ C_{ND|D}$, the result is $D_B(x)$ = D if x is positive and $D_B(x)$ = ND if x is negative. Cases 2 and 3 will have the same $D_B(x)$ as Case 1. However, if the cost ratios changed, this need not be the situation. For example, if $C_{D|ND} = 0.01\ C_{ND|D}$, then the RHS in equation (4) equals 100 for Case 1 and .01 for Case 2. So, Cases 1 and 2 would have different solutions.

For region B with $P(y = D) = 0.01$, in Cases 1 and 2, $D_B(x)$ = ND if x is positive and $D_B(x)$ = ND if x is negative. Because the prior probability assigned to observing a $y = D$ case is only 0.01, in Cases 1 and 2 we are not willing to label a positive test result as $y = D$. In Case 3, $D_B(x)$ = D if x is positive and $D_B(x)$ = ND if x is negative, so in Case 3 we are willing to label a positive test result as $y = D$ because of the high relative cost assigned to a false negative.

5. Conclusion and Summary

There is often considerable debate but little decided in a general argument recommending either the Bayesian approach or the frequentist approach to hypothesis testing. However, progress can be made on specific examples such those presented here.

Four summary comments follow related to why we believe that examples 3.3 and 4 are best handled using the Bayesian approach, there is essentially no difference in the frequentist and Bayes approaches for example 3.2, and that examples 3.1 and 3.4 are best handled using a frequentist approach.

1. In the *ID* example, example 3.1, conclusions depend on the particular alternative. That was illustrated in Table 1 using an alternative nearly equal to the null and an alternative far from the null. Because of the strong dependence on the magnitude of ID_{true} specified in the alternative hypothesis, for a complete analysis (not shown in this paper), the analyst must specify alternatives and probabilities for each. Better yet, a prior probability should be placed on each relevant alternative value for ID_{true}. Whether it is worthwhile to try to put prior probabilities on each alternative value is case-specific. And, for the *ID* example, it is almost certainly not worthwhile because of the more serious obstacle concerning the inability to specify a prior probability for $P(ID_{true} = 0)$.

Similarly, in Example 3.4, the frequentist framework and approach are the most natural and effective for lower limit of detection studies. We are not aware of any published Bayesian approaches to LLD problems and note that Lloyd (1968), which used a frequentist approach, is one of the most heavily cited publications in analytical chemistry.

2. Example 3.2 is safeguards-related verification measurements where the frequentist approach has a long tradition in safeguards because of the need to continually "trust but verify." Although previous inventory results are relevant in making conclusions for the current period if sequential testing is adopted, it is inappropriate to pool previous results in a manner that assumes the true percent defective p_D is constant over time. Therefore, the "uniform prior" Bayesian analysis is defensible, and the result is that the Bayesian sample size requirement is essentially the same as the frequentist sample size requirement.

However, verification measurements could be part of an internal monitoring of facility items for a different purpose than safeguards audits. For example, the monitoring could provide internal assurance that well-monitored stored items can still be measured effectively by the same assay method. This situation is much more akin to quality control situations in which previous performance (low observed defect rates in samples for example) is highly relevant for current inferences. In this case, it is more tenable to use a Bayesian approach that pools the results of previous samples with the current sample as a means to reduce future sample size requirements.

3. Example 3.3 involves constrained regression and the Bayesian approach is the logical foundation for enforcing constraints and associated uncertainties. Recall that this example is in the context of screening vehicles at ports entering the United States. Although we prefer a Bayesian approach for certain technical aspects (involving constrained regression) related to developing decision rules for releasing vehicles or sending them for further inspection, there is a largely unresolved aspect related to resource allocation for this type of problem. There are costs (typically unspecified) for the various mistakes (false alarms and false negatives) and there are prior probabilities for the rate of threat items, nuisance items (radioactive cargo such as cat litter). Perhaps these costs and probabilities could inform policy makers faced with deciding what types of equipment to install and what types of vulnerabilities to accept.

4. In the cancer screening example 4, the prior probability, $P(y = D)$ can easily be well estimated after sufficient data is accumulated in a country. Contrast that situation with the *ID* example. It is hard to imagine how we could gather years of data for a nuclear facility to support an estimate of $P(ID_{true} = 0)$. Reference 1 recommended that a Bayesian approach be used for testing $ID_{true} = 0$, but to date it has not been tried, and the paper met considerable opposition in the rejoinder section. One main reason for the opposition was the inability to specify the prior probability, $P(ID_{true} = 0)$. The inability to specify the prior probability is one opposition to many Bayesian analyses. However, depending on the goal of the analysis, it may be possible to choose a prior in a way that tends to err in a desired direction toward rejecting or accepting the null hypothesis.

It is sometimes thought that another reason for the difference between the cancer screening example and the *ID* example is that for the cancer example, the hypotheses are truly (simple) "point" hypotheses, stated as the null hypothesis: H_0: $y = ND$ versus the alternate hypothesis:

H_A: $y = D$.

Contrast that situation with the ID example. Certainly the true amount of missing nuclear material is rarely zero, even if no material is stolen. Trace amounts of material will typically be lost due to irrecoverable processing losses. The point null hypothesis H_0: $ID_{true} = 0$ is therefore more properly thought of as a fuzzy null: H_0: $|ID_{true}| < \epsilon$ for some small positive ϵ. However, Berger et. al. (1997) show that approximating a fuzzy null by a simple point null does not in general explain the source of discrepancy between Bayesian and frequentist approaches. In addition, analogously to the *ID* example, there could be "trace numbers of pre-cancerous cells" in some of the $y = ND$ cases. Perhaps a fuzzy null hypothesis such as H_0: "the number of pre-cancerous cells is less than a threshold" could be used in future diagnostic tests, but also in that case, the Bayesian approach would seem to be the more appropriate, so the "fuzzy" versus "point" null issue is not likely to be a reason to favor either a Bayesian or a frequentist approach.

In the cancer example, the expected misclassification cost was illustrated to construct a decision function, which forced the ratio of the costs of the two error types to be quantified. Though frequentists might object to the "need" to quantify that ratio, it is the ratio that justifies any particular procedure, regardless of whether a Bayesian approach is used. That is, any implemented procedure can only be optimal for some cost ratio, and refusal to specify the cost ratio cannot avoid this fact. In the ID example, political implications and practical impossibilities prevent assigning a prior probability π to the probability that the facility has $ID_{true} > 0$ (diversion). Therefore, although the cost f of false alarms is often considered when choosing a decision threshold and corresponding false alarm rate α, there is no attempt to separate the π and d (undetected diversion cost) terms in the expected cost given by Equation 3. This means that the frequentist can defend the practice of making reasonable but ad hoc, subjective choices for α and β in the context of *ID* evaluation.

References

1. Avenhaus, R., and M. Canty. 1999. Avoiding Useless Quantification, European Safeguards Research and Development Association. http://www.jrc.cec.eu.int/esarda/bulletin/bulletin_30/30ART_4.PDF
2. Berger, J., J.Boukai, Y. Wang. 1997. Unified Frequentist and Bayesian Testing of a Precise Hypotheses, *Annals of Statistics* 22, 1787-1807.
3. Burr, T., W. Charlton, and C. Nakhleh. 2005. Assessing Confidence in Inferring Reactor Type and Fuel Burnup: A Markov Chain Monte Carlo Approach, N*uclear Instruments and Methods in Physics Research* 555 (1-2), 426-434.
4. Currie, L. 1968. Limits for Qualitative Detection and Quantitative Determination: Application to Radiochemistry, *Analytical Chemistry* 40, 586-593, 1968.
5. Gattiker, J., and T. Burr. 2006. Bayesian Estimation of the Source and Suppression Effects in Vehicle Radiation Signatures, Los Alamos National Laboratory Unclassified Report LA06-3561, submitted to the *Journal of Nuclear Materials Management*, to be published in Volume 37(3).
6. Gelman, A., J. Carlin, H. Stern, and D. Rubin. 1995. *Bayesian Data Analysis,* Chapman & Hall: New York.
7. Gorbatenko, M., A. Zlobin, and V. Yuferev. 2006. Bayes' Approach to System Random Inspections for Nuclear Material Control and Accounting, *Journal of Nuclear Materials Management, Volume* 34(2).
8. Speed, T., and D. Culpin D. 1986. The Role of Statistics in Nuclear Material Accounting: Issues and Problems, *Journal of the Royal Statistical Society B.*

A Note from a Past President

John Lemming
INMM Chair 1989-1990

In 2004, I traveled to Orlando to attend the INMM annual meeting. Changing job responsibilities had caused me to miss the previous twelve annual meetings. I remembered that the annual meetings in the late 1980s into the early 1990s were exciting years to be involved with the INMM. The number of papers presented at annual meetings had increased to approximately 200 and we had moved beyond parallel sessions to concurrent sessions. As we grew it became harder and harder to find venues that accommodate our size meeting. I was curious to see the conference facilities and how the program committee allocated the meeting rooms.

The meeting was like a homecoming. I was able to renew old friendships and to meet new members and learn about their interests. I was not totally surprised because I had kept current with the growing membership, the chartering of new regional and student chapters, the number of papers presented at the annual meetings and the establishment of the technical divisions by reading the *Journal* and the proceedings from the annual meetings. What did impress me was the quality of the presentations and the enthusiasm and lively discussions that each of the technical divisions brought to their sessions. Many times, I wanted to attend more than one of the concurrent sessions at the same time. Two hundred and sixty-nine papers were presented compared to fifty-nine at my first INMM meeting in Seattle in 1976.

The 1976 meeting is memorable for me because I was invited to participate on the Technical Program Committee. As a technical program committee member, I learned that the INMM sponsored many other activities, where I could learn more about safeguards and which provided educational opportunities both for people seeking safeguards careers and for policy makers interested in nonproliferation. As an INMM member I had the opportunity to participate on an American National Standards Institute (ANSI) N-15 writing committee, to be one of the founding members of the Central Region Chapter that provided additional opportunities for professional development closer to home, to be a member of the Executive Committee and, finally, I had the privilege to serve as the chair in 1989 and 1990. These activities were the beginning of many lifelong friendships and an on-going learning process of the complexity of the safeguards issues.

Before my participation in the INMM, my professional experience had been in the laboratory developing nondestructive assay (NDA) measurements for domestic safeguards. Working with my INMM colleagues gave me a better appreciation of the multi-disciplinary character of an integrated safeguards system. I learned how my NDA results would be used for accounting and how material control and accounting (MC&A), physical protection (PP), the protective force (Pro-Force), waste management, transportation and international safeguards all contributed to the integrated system that mitigates nonproliferation. The INMM provided me with opportunities to interface with members from each of those disciplines that I would not have had through my work environment alone. The INMM helped me to become a better spokesperson for advocating nonproliferation.

Since 1958 the INMM has provided an open forum to discuss all facets of the technical and political issues that impact the credibility of nuclear material accounting and security systems from both domestic and international perspectives. It is encouraging that today, the INMM and its members continue to lead the way in developing and implementing strategies to assure that nuclear material is adequately controlled. In addition, the Institute provides educational opportunities for its members and others interested in improving the technologies used to protect against the potential theft of nuclear materials and nuclear proliferation.

Becoming an active member of the INMM has enriched my life both professionally and personally. I will never regret accepting the invitation I received in 1976. If you are not currently active in the INMM, you are invited to take advantage of a similar opportunity to make friends and grow professionally. Both you and the INMM will accrue substantial benefits.

Book Review

By Walter Kane
JNMM *Book Review Editor*

Deliberative Democracy for the Future: The Case of Nuclear Waste Management in Canada. Genevieve Fuji Johnson. Univeristy of Toronto Press, Inc. 2008.

ISBN 978-0-8020-9607-4

With our current, compelling need for new, affordable, carbon-free sources of electrical energy, it is inevitable that we will experience a "nuclear renaissance" with the construction of a number of new power plants and the expansion of related industries. A major obstacle in the way of this necessary development is the perception on the part of the public that nuclear energy is inherently dangerous and destructive to the environment, i.e., "There is no way to deal with nuclear waste!" In this context, Genevieve Fuji Johnson's book "Deliberative Democracy for the Future: The Case of Nuclear Waste Management In Canada," has a great deal to contribute. Johnson, an assistant professor of political science at Simon Fraser University in Vancouver, Canada, discusses in detail the public deliberations that took place in Canada between 1989 and 1997 on the proposal by the Canadian government to dispose of several thousand spent fuel elements by means of deep geological placement in the Canadian Shield. These "Public Scoping Meetings" were held throughout Canada under the aegis of an independent assessment panel chaired by Blair Seaborn. Over a period of several years more than 500 participants contributed to the discussions. Inevitably, these participants divided themselves into two coalitions, one putting its faith in technical risk assessment, while the other coalition argued that safety cannot be determined strictly by this process. The first coalition argued that government and industry should have sole responsibility for the management of nuclear waste while the second coalition argued that there should be broad public participation in the process. At the end of this lengthy deliberative process the responsibility for nuclear waste was put totally in the hands of industry and government.

In subsequent chapters the author goes into a detailed discussion of the ethical issues involved in the management of nuclear waste: These include future generations, safety and risk, burdens and benefits, inclusion and empowerment, and accountability and oversight. Much of this material will be new to the reader; the important conclusion is the recommendation that "deliberative democracy" is the preferred process for achieving public acceptance of any new technology. On practical terms this implies thorough public discussions with widespread participation by citizens from various communities and a serious effort to arrive at a consensus on the technology in question. In this process it must be remembered that different individuals will possess different values, backgrounds, concerns, and interests. In particular, many members of the public are not convinced that probabilistic risk analysis should have the last word, especially, for example, in the case of isotopes with half-lives of many thousands of years. The author recommends strongly that this process should continue until a consensus is achieved, reminiscent of the exclamation by Jacob while wrestling with an angel, "I will not let thee go until thou bless me!" It is further recommended that, unlike in the case of the Seaborn Panel, that members of the public continue to participate in the oversight and management of the technology, thus building a constituency on the part of the public and a sense of empowerment.

These ideas should be directly applicable in the near future to public discussion on the expansion of nuclear energy, and in particular, on the management of nuclear waste. In the latter case, it is evident that reprocessing, rather than long-term storage, has not only technical advantages but also the advantage that it addresses public concerns about the hazards of long-lived isotopes.

U.S. Department of Energy Awards Contract for Management and Operating Contractor Support for Yucca Mountain

In October 2008, the U.S. Department of Energy (DOE) awarded a $2.5 billion management and operating (M&O) contract to USA Repository Services (USA-RS), a wholly-owned subsidiary of the URS Corporation. USA-RS will be supported by principal subcontractors Shaw Environmental and Infrastructure, Inc., and AREVA Federal Services, Inc.

USA-RS will provide mission support to the Office of Civilian Radioactive Waste Management (OCRWM) for the Yucca Mountain Project.

Key scope activities under this new M&O contract are:

- providing management expertise and support for the completion of repository design;
- addressing questions or requests for additional information from the U.S. Nuclear Regulatory Commission (NRC) on the DOE's License Application and supporting DOE's activities in the subsequent NRC licensing process;
- operating the Yucca Mountain site;
- providing construction management and integration support.

As awarded, this contract has a five-year period of performance with a potential five-year option period. If fully exercised, this contract will continue through March 31, 2019.

After the transition activities are completed, USA-RS will assume responsibility for full performance on April 1, 2009. A Web site providing information on the new contract will be set up prior to transition and will be accessible from the OCRWM Web site at http://www.ocrwm.doe.gov/.

IAEA and International Science and Technology Center Sign Cooperative Agreement

In October 2008, the IAEA and the International Science and Technology Center (ISTC) signed an agreement that calls for increased cooperation between the two organizations. The memorandum of understanding seeks to amplify their collaboration in the research and development of applications and technology that could contribute to the IAEA's activities in the fields of verification and nuclear security, including training and capacity building.

IAEA Safeguards Director of Technical Support Nikolay Khlebnikov and ISTC Executive Director Adriaan van der Meer signed the Agreement at IAEA headquarters in Vienna on October 22, 2008.

The ISTC is an intergovernmental organization dedicated to nonproliferation work in Russia and the other countries of the Commonwealth of Independent States. Its main activity is to fund research projects and seek to bring industrial and governmental agencies into contact with the high-level expertise available in Russia and other countries of the Commonwealth of Independent States.

IAEA Director General Observes NEA 50th Anniversary, Lauds Five Decades of NEA-IAEA "Nuclear Partnership"

Fifty countries have informed the International Atomic Energy Agency (IAEA) that they are considering introducing nuclear power, IAEA Director General Mohamed ElBaradei told a meeting marking the fiftieth anniversary of the Organization for Economic Cooperation and Development Nuclear Energy Agency (OECD NEA) in Paris in October 2008.

"When I spoke here ten years ago as the NEA turned forty, nuclear power had stopped growing in Western Europe and North America. The outlook was uncertain in other parts of the world. Public perceptions were mainly negative. When we talked about transferring nuclear technology to developing countries, we generally meant applications in medicine and industry, not nuclear power.

"By contrast, at the IAEA General Conference in Vienna two weeks ago, so many of our member states announced that they were considering the introduction of nuclear power that I stopped counting. Most of them were from the developing world. In the OECD, countries that used to talk about phasing out nuclear power seem to have changed their minds, while others are planning new reactors."

"Change is definitely in the air," he said. He also stated that much is to be done if nuclear power's future is to be "safe, proliferation-resistant, and cost-effective." And he called upon OECD member countries and "nuclear newcomer" states to work responsibly together in the areas of nuclear safety and nuclear power.

ITER and IAEA to Enhance Cooperation on Fusion Research

The IAEA and the International Thermonuclear Experimental Reactor (ITER) Organization signed an agreement in October 2008 that will enhance the research of fusion, a form of nuclear energy created by the merging of light atoms.

The cooperation agreement is aimed at strengthening the working relationship between both organizations "with a view to facilitating the effective attainment of the objectives set forth in the IAEA Statute and the ITER Agreement."

Yury Sokolov, deputy director general of the International Atomic Energy Agency (IAEA), and director general of the ITER Organization Kaname Ikeda signed the agreement on the opening day of the *22nd IAEA Fusion Energy Conference,* held in Geneva, Switzerland, in October 2008.

The IAEA has been closely involved with ITER since its inception, as the previous ITER cooperation phases and the ITER negotiations were held under its auspices. The IAEA Director-General is also the Depository of the ITER Agreement.

According to the Cooperation Agreement, both organizations will exchange information regarding the study and potential application of fusion energy and will participate in each other's meeting. These will include ITER Council meetings and Annual Conferences of the IAEA, as well as its scientific and technical committees.

The IAEA and the ITER Organization will also cooperate on training, publications, organization of scientific conferences, plasma physics and modeling, and fusion safety and security.

The cooperation agreement is also expected to broaden the reach of fusion research into countries that do not currently have fusion programs but may wish to participate in fusion science and research in the future.

The agreement entered into force upon signature and will be communicated to the Secretary General of the United Nations for registration and publication.

U.S. Additional Protocol Enters into Force

Five Nuclear-Weapon States Now Have APs in Place

An Additional Protocol to the nuclear safeguards agreement (AP) between the IAEA and the United States entered into force on January 6, 2009.

U.S. Ambassador Gregory Schulte formally handed over the notification of the completion of the US´ ratification procedures to IAEA Director General Mohamed ElBaradei, marking the effective date for the entry into force of the AP for the country.

With the entry into force of the U.S. AP, all five nuclear-weapon states party to the Treaty on the Nonproliferation of Nuclear Weapons (NPT) have fulfilled their undertaking, assumed at the time of approval by the IAEA Board of Governors of the Model Additional Protocol in 1997, to conclude such APs.

The entry into force of the U.S. AP brings the number of states with APs to eighty-nine and contributes to efforts aimed at achieving universal application of APs.

U.S. And Russia Complete Nuclear Security Upgrades Under Bratislava Initiative

The U.S. Department of Energy in December 2008 delivered the Bratislava Nuclear Security report to the White House, which detailed the status of work agreed to by Presidents Bush and Putin in Bratislava in 2005. U.S. and Russian officials from the U.S. Department of Energy's National Nuclear Security Administration (NNSA), the U.S. Department of Defense, the Russian Ministry of Defense and State Atomic Energy Corporation (Rosatom) reviewed work to complete nuclear security upgrades in Russia at meetings in Moscow last week. Building on this success, both countries will continue to actively pursue additional Presidential objectives.

The Bratislava Nuclear Security Initiative was launched by then-President Bush and then-President Putin during their meeting in Bratislava, Slovak Republic in February 2005. Both sides agreed to enhanced cooperation in five key areas: upgrading security of nuclear facilities, expanding emergency response, enhancing nuclear security culture, accelerating research reactor conversions and fuel returns, and sharing best practices. Nuclear security upgrades were accelerated by two years and will be completed by the end of 2008.

The upgrades included in the Bratislava Nuclear Security Initiative represented the vast majority of such work in Russia. Some additional cooperative work that was agreed to after 2005 will continue until 2012. At the same time, the United States and Russia are putting in place the necessary elements to ensure the long-term sustainability of these upgrades.

In addition, the United States and Russia continue to cooperate to fulfill the Bratislava commitments to convert research reactors internationally fueled with highly enriched uranium (HEU) to low enriched uranium fuel and to return all Russian-origin HEU fresh and spent nuclear fuel stored outside research reactors to Russia by 2010. To complement the physical security upgrades at nuclear weapons storage sites, the U.S. also assisted the Russian Ministry of Defense in automating its nuclear weapons inventory management system and continues to work jointly to enhance the secure transportation of nuclear weapons from operational sites to dismantlement facilities and to centralized storage.

GNEP Nations Hold Infrastructure Development Working Group Meeting

In December 2008, representatives from the U.S. Department of Energy (DOE) participated in the third Global Nuclear Energy Partnership (GNEP) Infrastructure Development Working Group (IDWG), underscoring the Department's commitment to ensuring that global expansion of civilian nuclear power is done safely and securely, while reducing the risk of nuclear proliferation and responsibly managing waste. The IDWG, held December 8th and 9th in Vienna, Austria, includes more than seventy participants from twenty-two countries working to support the sharing of educational resources, the promotion of technical educational opportunities and the establishment of new programs by which nuclear energy issues can be properly supported by trained, educated, and qualified personnel.

During the IDWG meeting on December 8, participating nations identified priorities and activities for the working group to pursue in 2009 and continued to express support for critical infrastructure needs identified in 2008—such as human resource development, legal and regulatory framework development and sharing of lessons learned. In addition, the IDWG held a workshop to address the challenges of managing radioactive waste in ways that address the common interests and concerns of the GNEP partners and that are consistent with internationally-accepted principles of radioactive waste management and safety standards. The workshop was a result of GNEP partners' unanimous support for a proposal by the United Kingdom that GNEP seek to facilitate

strategies for the responsible management of nuclear wastes.

On December 9, the IDWG held a Resources and Gaps Workshop which focused on providing human resource development support in areas that include stakeholder engagement, legal and regulatory frameworks and reactor siting. The workshop brought together experts from around the world in government, industry and nongovernmental organizations to share information and discuss ways in which GNEP partners can complement and enhance other efforts to promote human resource development solutions.

The new IDWG activities are pursuant to Secretary Samuel W. Bodman's participation in the October 1, 2008, GNEP Ministerial Meeting in Paris, France, where GNEP partner countries discussed the importance of multilateral engagement in the area of infrastructure development to ensure that the expansion of the use of nuclear energy around the world is done in a safe and secure manner. At the Paris meeting there was agreement to engage industry and the educational community in GNEP endeavors.

GNEP is a partnership of 25 nations joined in an effort to collectively address the challenges confronting countries that are maintaining, expanding or starting nuclear power programs.

AEA Completes Third Mission to Kashiwazaki-Kariwa Nuclear Power Plant

An IAEA-led team of international experts has completed its third mission, at the invitation of the government of Japan. This follow-up mission continued to share the lessons learned from the effects of the July 2007 earthquake of the Kashiwazaki-Kariwa nuclear power plant.

The mission received further evidence confirming the findings of previous missions regarding the safe performance of the plant during and after the earthquake.

The mission found that there is consensus in the scientific community about the causes of the unexpectedly large ground motions experienced at the plant site during the July 2007 earthquake and, consequently, it has been possible to identify the precautions needed to be taken in relation to possible future events.

These precautions were based on extensive studies and assessments conducted by a number of specialized institutions and experts in different fields. The necessary upgrades and actions were consequently defined and are being implemented by the Japanese utility for both safety and non-safety related components at the nuclear power plant.

The lessons learned from the Kashiwazaki-Kariwa experience has also contributed to the development of IAEA Safety Standards related to seismic safety. These standards are expected to be released shortly.

The mission´s report will be provided to the Japanese Nuclear and Industrial Safety Agency (NISA) and will be made publicly available in January 2009.

The IAEA conducted two previous missions to the Kashiwazaki-Kariwa NPP in August 2007 and January and February 2008.

The experience from recent strong seismic events and the lessons learned through the missions to Kashiwazaki-Kariwa NPP have led to the establishment of an International Seismic Safety Centre (ISSC) at the IAEA that is working as a focal point for seismic safety-related information about nuclear installations.

Calendar

March 10–11, 2009
3rd Annual Workshop on Reducing the Risk from Radioactive and Nuclear Materials
Double Tree Albuquerque
Albuquerque, NM USA
Sponsor: Institute of Nuclear Materials Management
Contact: INMM
+1-847-480-9573
Fax: +1-847-480-9282
E-mail: inmm@inmm.org
Web Site: www.inmm.org/meetings

July 12–16, 2009
50th INMM Annual Meeting
JW Marriott Starr Pass Resort
Tucson, AZ USA
Sponsor: Institute of Nuclear Materials Management
Contact: INMM
+1-847-480-9573
Fax: +1-847-480-9282
E-mail: inmm@inmm.org
Web Site: www.inmm.org/meeting

July 11–15, 2010
51st INMM Annual Meeting
Marriott Baltimore Waterfront Hotel
Baltimore, MD USA
Sponsor: Institute of Nuclear Materials Management
Contact: INMM
+1-847-480-9573
Fax: +1-847-480-9282
E-mail: inmm@inmm.org
Web Site: www.inmm.org/meetings

Advertiser Index

INMM Membership Application

MEMBERSHIP

All information should be printed or typewritten.

Name _____ Date _____

Employer _____ Title _____

Address

Address _____

City _____ State/Province _____ Country _____ Zip _____

Telephone _____ Fax_____ E-mail _____

If you would like your INMM mail sent to an alternative address, please indicate preferred mailing address:

Address _____

City _____ State/Province _____ Country _____ Zip _____

Occupation

❑ Commercial Utility ❑ Government Contractor ❑ Nuclear Material Processing
❑ Equipment Manufacturer ❑ Government or International Agency ❑ Research or Consulting
❑ Other (describe): _____

Field(s)/Subject(s) of expertise _____

Total number of years work experience in nuclear materials management field(s) _____

Education (If you are applying for a student membership, indicate the year that you anticipate receiving your degree)

College/University Major/Degree Year Degree Obtained/Expected

1. _____

2. _____

3. _____

If you are applying for a student membership, provide contact information for a faculty advisor to verify your full-time status:

Name _____ Telephone _____ E-mail _____

Membership Type Desired

❑ Student $20
❑ Regular $50

Sustaining:
❑ 0 – 19 employees $250
❑ 20 – 49 employees $500
❑ 50 or more employees $750

From the categories listed below, please indicate your top 3 areas of interest within INMM (1 being the greatest interest):

___ International Safeguards
___ Materials Control and Accountability
___ Nonproliferation & Arms Control
___ Packaging & Transportation
___ Physical Protection
___ Waste Management

Membership in Other Scientific and Technical Societies (Attach additional sheet if necessary)

Society Names and Membership Grades _____

Signature _____
PAID BY: ❑ Check ❑ MasterCard ❑ VISA ❑ American Express ❑ Diners Club

Card No. _____ Exp. Date _____

Complete the application (keep a copy for your records) and mail or fax it with membership dues to:

INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT
111 Deer Lake Road, Suite 100 • Deerfield, Illinois 60015 USA
+1-847-480-9573, Fax: +1-847-480-9282
E-mail: inmm@inmm.org • Website: www.inmm.org

INMM
INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT

Scintillation Detector-Based On-Line Gamma-Ray Monitors?

What's missing from this picture?

Absolutely Nothing!

The ORTEC digiBASE is your answer to the simple implementation of enrichment or process radiation monitors:

- A complete high performance digital spectroscopy system built into a standard 2" PMT base
- 1024 channels
- Digital gain stabilizer
- PHA and List mode
- Auxiliary counter/gate input
- 1200 V bias supply
- Standard 14-pin PMT base
- USB communications for today's PC
- ORTEC's legendary MAESTRO-32 MCA software
- Programmer's Toolkit option

Just because you need to do it yourself does not mean you can't use a little help.

For on-line process monitoring, the ORTEC digiBASE is a great place to start.

- Safeguards
- Fuel Manufacture
- Reprocessing
- Environmental Monitoring
- Down Blending

801 South Illinois Ave., Oak Ridge, TN 37831-0895 U.S.A. • (865) 482-4411 • Fax (865) 483-0396 • ortec.info@ametek.com

For International Office Locations, Visit Our Website

www.ortec-online.com

ORTEC®

AMETEK®