JNMM
Journal of Nuclear
Materials Management

Published by the Institute of Nuclear Materials Management ■ Volume XXVIII, Number 3 ■ Spring 2000

JNMM

Technical Editor
Dennis Mangan

Associate Editors
Gotthard Stein and Bernd Richter, *International Safeguards*
Dennis Wilkey, *Materials Control and Accountability*
Jim Lemley and Mike Heaney, *Nonproliferation and Arms Control*
Scott Vance, *Packaging and Transportation*
Janet Ahrens, *Physical Protection*
Pierre Saverot, *Waste Management*

Book Review Editor
Walter R. Kane

INMM Communications Committee
Cathy Key, *Chair*
Paul Ebel, *Oversight*
Charles E. Pietri, *Annual Meeting*

INMM Executive Committee
Debbie Dickman, *President*
J.D. Williams, *Vice President*
Vince J. DeVito, *Secretary*
Robert U. Curl, *Treasurer*
Obie Amacker Jr., *Past President*

Members At Large
Paul Ebel
Sharon Jacobsen
John Matter
Dave Shisler

Chapters
Chris Pickett, *Central*
Kenneth Sanders, *Northeast*
Brian Smith, *Pacific Northwest*
Obed Cramer, *Southeast*
Chad Ollinger, *Southwest*
Syunji Shimoyama, *Japan*
Byung-Koo Kim, *Korea*
Gennady Pshakin, *Obninsk Regional*
Yuri Volodin, *Russian Federation*
Jaime Vidaurre-Henry, *Vienna*

Headquarters Staff
John Waxman, *Executive Director*
Rachel Airth, *Account Manager*
Patricia Sullivan, *Managing Editor*
Mark Johnson, *Layout*
Lyn Maddox, *Manager, Annual Meeting*
Nadine Minnig, *Accounting*
Jill Hronek, *Advertising Director*

International Advertising Sales Representative
Bill Kaprelian, Kaprelian & Co., 914 W. Main St., St. Charles, IL 60174 U.S.A.
Phone, 630/584-5333; Fax, 630/584-9289

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 and safeguards of nuclear materials.

SUBSCRIPTION RATES: Annual (United States, Canada, and Mexico) $100.00; annual (other countries) $135.00 (shipped via air mail printed matter); single copy regular issues (United States and other countries) $25.00; single copy of the proceedings of the Annual Meeting (United States and other countries) $175.00. Mail subscription requests to *JNMM*, 60 Revere Drive, Suite 500, Northbrook, IL 60062 U.S.A. Make checks payable to INMM.

ADVERTISING, distribution, and delivery inquiries should be directed to *JNMM*, 60 Revere Drive, Suite 500, Northbrook, IL 60062 U.S.A., or contact Jill Hronek at 847/480-9573; fax, 847/480-9282; or E-mail, inmm@inmm.org. Allow eight weeks for a change of address to be implemented.

Opinions expressed in this publication by the authors are their own and do not necessarily reflect the opinions of the editors, Institute of Nuclear Materials Management, or the organizations with which the authors are affiliated, nor should publication of author viewpoints or identification of materials or products be construed as endorsement by this publication or by the Institute.

CONTENTS

Volume XXVIII, Number 3 • Spring 2000

PAPERS

INMM NEWS

ANNOUNCEMENTS

Can We Form Stronger Networks in Nuclear Materials Management and Nonproliferation?

The late Willy Higgenbotham, from Brookhaven National Laboratory, was a long-time contributor to nonproliferation programs and one of the pioneers of the INMM. He made the following statement in a *Journal of Nuclear Materials Management* column in the early 1980s :

> *Safeguarding nuclear materials is an international undertaking on behalf of society as a whole. The key is to agree on what we are trying to do, and to do it together.*

Those words are even more meaningful today as we see the global environment changing and those of us engaged in nuclear materials management professions draw closer together in our common quest. Many of the issues facing INMM's founders more than 40 years ago are still prevalent today. In addition, many other new and challenging issues are confronting us. As weapons dismantlement activities increase, and material disposition alternatives are evaluated and implemented, there will be many more challenges facing us. Safeguards and nonproliferation are issues of global interest and concern.

Many political, governmental, and non-governmental organizations have wrestled with and continue to wrestle with these ideas. The amount of international cooperative efforts has increased significantly in the last few years. These expanding networks have played an important role in promoting technical cooperation, exchange information, and provide the experience necessary to resolve important issues.

For several years the INMM has been cooperating with ESARDA, the International Atomic Energy Agency, the American Nuclear Society, and other organizations to organize seminars, workshops and meetings on topics of safeguards and nonproliferation. These events provide unique opportunities for interdisciplinary technical exchanges involving a large number of stakeholders.

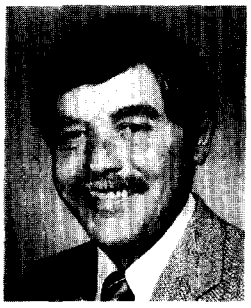
These national and international organizations are dedicated to solving problems related to responsible nuclear materials management. Are there ways we can encourage further cooperation and communication among our professional colleagues? Can we find additional ways to join together to positively influence events in the field of safeguards and nonproliferation?

I recently returned from an international conference on nuclear materials protection, control and accounting, held in Obninsk, Russia. This conference — co-sponsored by the INMM — was attended by representatives from all over the world. This issue was raised again and again — in open forum as well as personal conversations.

I am interested in hearing your suggestions and ideas regarding ways the INMM could link more closely with our national and international colleagues, to improve coordination and provide expanded forums for sharing innovative ideas and technologies. Please feel free to contact me to discuss your thoughts.

Debbie Dickman
INMM President
Pacific Northwest National Laboratory
Richland, Washington U.S.A.
Phone: 509/372-4432
Fax: 509/372-4559
E-mail: debbie.dickman@pnl.gov

Presenting a "Variety Pack" of Technical Papers



I tried in vain to have someone write a predictive article on issues to be discussed at the 2000 NPT review conference being held in New York City this April and May. I thought such an article would have been useful to capture perhaps the international political flavor that has evolved over the decision by the United States not to ratify the Comprehensive Test Ban Treaty and the rumblings that are paramount regarding the present U.S. views on the antiballistic missile treaty and its hindering the U.S. ability to protect itself against certain perceived threats, the nuclear tests by India and Pakistan, and other world events that have occurred since the 1995 review conference. Perhaps I can find someone to write a summary after-the-fact article. Any volunteers?

This year's 41st Annual Meeting of the Institute should prove to be an interesting one. Pierre Goldschmidt, the deputy director for safeguards for the International Atomic Energy Agency, will be our plenary speaker. I first met Goldschmidt almost immediately after he assumed his new position. I was delighted when he told me that more than one person at the IAEA had informed him that his support for the Institute needed to be a high priority item for him. Last year was the first year he attended the annual meeting, and if I recall correctly, he was present for the entire meeting. I'm sure his opening remarks at this year's meeting will be very informative.

This issue of the Journal again has a variety pack of papers. Rod Martin from Pacific Northwest National Laboratory, in his article, Performance Validation of Monitoring Systems for Strengthened Safeguards, suggests extending the usual role of remote monitoring (normally associated with containment and surveillance) to perhaps include process monitoring or the monitoring of process operations. As do many, I believe remote monitoring can play an effective role in international safeguards. Although it has not yet been implemented, except for some limited demonstrations and evaluations, progress is being made in this area.

In the second article, A Simple Evaluation Model on the Effectiveness of Integrated Safeguards Implementation, author Hiroshi Matsuoka, of the Japan Atomic Energy Research Institute, proposes a simple, practical model to evaluate the effectiveness of integrated safeguards implementation (INFCIRC/153 and INFCIRC/540 combined). It has been awhile since I have given thought to truth values.

Roger Johnson and Anthony Garcia of Los Alamos, in their paper, An Annotated Taxonomy of Tag and Seal Vulnerabilities, define and discuss 105 different generic attacks on seals and 91 attacks on tags as a structured approach to characterize the weaknesses of tags and seals (or alternatively, the tags and seals robustness). They identify 11 major scenarios for attempting to defeat a seal and two for tags. These major scenarios are further structured by specific attacks. Their approach could bring further structured thinking to vulnerability assessments.

Dennis Togo from the University of New Mexico and Claude Potter from Sandia National Laboratories discuss "activity-based costing" and focus their efforts on developing costs for physical protection upgrades. They consider a baseline case and then examine the costs for three different approaches for upgrading the security needs. One of their conclusions, which they acknowledge should be obvious, is the fact that security considerations must be an integral part of the design of a new facility.

The final paper comes from our friends in the Russian Federation, particularly the Institute of Physics and Power Engineering at Obninsk. V. Piksaikin, A. Goverdovski, G. Pshakin, and S. Isaev discuss methods for measuring trace levels of fissionable nuclides using the delayed neutron counting technique. This technology could have application in the context of the Additional Protocol for the application of IAEA safeguards in evaluating environmental samples taken to identify undeclared activities such as enrichment operations or reprocessing operations.

As always, I welcome any comments or suggestions you may have. I plan to be at the Annual Meeting in New Orleans. Feel free to approach me with ideas for the Journal.

Dennis L. Mangan
JNMM Technical Editor
Sandia National Laboratories
Albuquerque, New Mexico, U.S.A.
Phone: 505/845-8710
Fax: 505/844-6067
E-mail: dlmanga@sandia.gov

In Changing Political Climate, INMM Annual Meeting Is More Important Than Ever

As the international political climate continues to change, this is a particularly important time for the exchange of technical information on many issues facing the nuclear materials management community. The Institute of Nuclear Materials Management's 41st Annual Meeting, July 16–20, 2000, is an excellent forum for this kind of exchange of ideas.

The meeting will be held at the New Orleans Riverside Hilton in New Orleans, Louisiana, U.S.A.

The technical program at this meeting will appeal to nuclear materials professionals in materials control and accountability, physical protection, international safeguards, nonproliferation and arms control, packaging and transportation, and waste management. More than 300 papers will be presented during 43 sessions. Topics of immediate interest will be discussed during these formal presentations, as well as during informal meetings of attendees. The program, which was arranged by the six technical divisions of the Institute in cooperation with the technical program committee, chaired by Charles E. Pietri, will be timely and informative.

The opening plenary session will be held Monday, July 17, and the closing plenary session will be held Thursday, July 21.

In addition to the formal technical program, the INMM Annual Meeting also provides attendees an opportunity to conduct business with one another productively and cost-effectively. This one meeting in Louisiana can put you in contact with other nuclear materials management professionals from around the United States and the world.

In addition, each of the INMM technical divisions — Materials Control and Accountability; Physical Protection, Nonproliferation and Arms Control; Packaging and Transportation; International Safeguards; and Waste Control — will conduct meetings on Sunday, July 16. These special meetings are open to all.

The New Orleans Riverside Hilton has excellent conference facilities that allow you to move quickly from exhibits to technical and poster sessions. In addition, there's plenty of space to hold informal discussions and impromptu meetings. The Hilton is connected to the Riverwalk Festival Marketplace and is only three blocks away from the historic French Quarter.

For more information on the Annual Meeting or to request registration materials, visit the INMM Web site at www.inmm.org or call INMM Headquarters at 847/480-9573.

James D. Williams
Vice President, INMM
Sandia National Laboratories
Albuquerque, New Mexico U.S.A.

ANS Honors INMM's Ruth Kempf

C. Ruth Kempf, chair of the INMM's Nonproliferation and Arms Control Technical Division, was honored by the American Nuclear Society for her contributions to nuclear safety and nonproliferation. Kempf received the Women's Achievement Award, which is given each year to recognize outstanding personal dedication and technical achievement by a woman for work she has performed in the fields of nuclear science, nuclear engineering, research or education.

Kempf is deputy chair of Brookhaven National Laboratory's Department of Advanced Technology. Her technical work focuses on nonproliferation, including the U.S.-Russian program to safeguard weapons-useable nuclear materials.

From 1990 to 1992, she was a technical advisor to the U.S. Ambassador to the Conference on Disarmament in Geneva. In 1995, she served on a presidential advisory panel to produce a classified report on U.S.-Russian nuclear security issues, which has influenced U.S. policy developments in this area.

Kempf holds bachelor's degrees in chemistry and German, a master's degree in radioanalytical chemistry, and a Ph.D. in physical chemistry, all from Rensselaer Polytechnic Institute. She was an assistant professor of chemistry at Fort Lewis College in Durango, Colorado, before joining BNL in 1982.

Kempf expressed her appreciation to the ANS for showcasing the accomplishments of women in technical fields. "It is refreshing to be called up from the depths of involvement in work to receive this type of recognition," she said.

Technical Division Reports

International Safeguards

The next meeting of the INMM International Safeguards Division will be held on Friday, May 12, 2000, from 9:30 a.m. to noon, at the Hotel Astron, Dresden, Germany, the site of the 22nd ESARDA annual meeting. The suggested discussion topics for this meeting are:

- the NPT review conference
- the ESARDA meeting topics, including the IAEA's Integrated Safeguards System
- future R&D to support international safeguards.

It should be noted that the attendance in the ESARDA meeting is limited to 150 participants, based on the criterion first come, first served.

Planning continues for the Third Joint INMM/ESARDA Workshop on Science and Modern Technology for Safeguards, which will be held in Tokyo, Japan, November 13–16, 2000. This workshop will be hosted by the Japan and Korea chapters of the INMM and the Australian Safeguards and Nonproliferation Office. The workshop will be open to members of the two organizations, as well as to others in the scientific and international safeguards community.

Cecil Sonnier
Chair, International Safeguards Division
Jupiter Corp.
Albuquerque, New Mexico U.S.A.

Nonproliferation and Arms Control

The Nonproliferation and Arms Control Technical Division of INMM, in cooperation with the Non-Proliferation Project of the Carnegie Endowment for International Peace, will host a special one-day seminar on Russian nuclear security, programs, and prospects. Speakers from Congress, the departments of State, Defense, and Energy, program participants, academia, and the NGO community will take part.

The morning segments will comprise two panels, focused on major sectors of Russian nuclear security, the "brain drain" or weapons knowledge proliferation, and safeguarding nuclear weapons and fissile materials.

The luncheon speaker will be U.S. Sen. Pete Domenici (R-New Mexico).

The afternoon will be devoted to forward-looking, "visionary" ideas and approaches to these two sectors and to other relevant aspects of this thorny problem. Speakers will identify the technical, implementation and policy hurdles presented by their suggested paths forward.

The seminar took place Wednesday, April 26, 2000, at the Hyatt on Capitol Hill in Washington, D.C.

Ruth Kempf
Chair, Nonproliferation and Arms Control Division
Brookhaven National Laboratory
Upton, New York U.S.A.

Committee Reports

Membership Committee

The membership status of the Institute of Nuclear Materials Management as of March 1, 2000, is as follows:

676	Regular Members
72	Senior Members
3	Senior Emeritus Members
19	Fellows
7	Fellow Emeritus Members
2	Student Member
17	Emeritus Members
26	Sustaining Members (some of these overlap with other categories)
1	Honorary Member
	Total Membership: 823

The Membership Committee is currently comprised of Nancy Jo Nicholas (chair), Roy Cardwell, Jill Cooley, Bob Curl, Vince DeVito, Al Garrett, Michelle Kazanova, Larry Kwei, Bruce Moran, Takeshi Osabe, Don Six, and Scott Vance.

The membership directory was mailed in late April. Members who haven't received their copies should contact INMM Headquarters.

Cathy Key and the communications team are working on a new design and text for the membership brochure. Until they are ready, headquarters will reprint limited numbers of the current brochure as needed.

A new member of the Membership Committee, Scott Vance of JAI, has volunteered to take the lead in encouraging student participation. He plans to work with the regional and local chapters to develop specific proposals to encourage student involvement in INMM, specifically encouraging student papers and scholarships for the annual meeting.

Nancy Jo Nicholas
Membership Committee Chair
Los Alamos National Laboratory
Los Alamos, New Mexico U.S.A.

Chapters

Vienna Chapter

Preparations are under way for the next INMM safeguards symposium, which will take place on May 15, 2000, at the Vienna International Center. Many papers on safeguards-related topics will be presented, including those papers that are selected for the INMM 41st Annual Meeting.

Abstracts were forwarded for consideration for the INMM 41st Annual Meeting. This year, all the abstracts submitted have already received sponsorship from the Department of Safeguards. Therefore, participation of the presenters can be assured.

John Carlson, director general of the Australian Safeguards and Non-Proliferation Office, was the guest speaker at the last luncheon that took place on November 17, 1999. Carlson spoke on the commonalities and differences of the Chemical Weapons Convention and the Non-Proliferation Treaty, and discussed the Organization for the Prohibition of Chemical Weapons located at The Hague, Netherlands.

The Vienna Chapter was invited to participate in the INMM Government-Industry Liaison Committee. Anita Nilsson was nominated as the Vienna Chapter representative. Nilsson is head of the Office of Physical Protection and Material Security reporting to the deputy director general of safeguards and is currently serving as vice president of the Vienna Chapter.

Jaime Vidaurre-Henry
President, INMM Vienna Chapter
IAEA
Vienna, Austria

Russian Federation Chapter

The Russian Federation Chapter members concentrated their activities on three major areas. These are:

- participation in the meeting organized or supported by INMM;
- participation in the U.S.-Russian projects within the government-to-government, Minatom-DOE, Gosatomnadzor-DOE, MVD-DOE, MOD-DOE, Gosatomnadzor-NRC and Kurchatov Institute-DOE agreements and arrangements;
- participation in international cooperation programs in the area of MPC&A, nonproliferation and arms control, nuclear materials transportation and management, waste managements, and disposal.

During 1999, the Russian Federation Chapter admitted five new members representing the Russian nuclear and research institutions and one from the governmental agency. The Chapter however lost two very active members who passed away. As of Feb. 24, 2000, the Russian Federation Chapter had 21 members from 14 governmental and nongovernmental organizations.

On Nov. 19, 1999, the Russian Federation Chapter held its annual meeting in Moscow. The meeting served several purposes including reviewing the annual report provided by Alexander Izmailov, then chair of the Russian Federation Chapter on the participation of the Russian Federation Chapter members in INMM activities; electing executive officers for 2000; admitting new chapter members; and discussing and planning actions to inform various governmental, scientific, and public organizations on INMM activities, objectives, and achievements.

The new Russian Federation Chapter officers for 2000 are:

continued on page 13

Encouraging the Advancement of Nuclear Materials Management: 3rd Workshop on Science and Modern Technology for Safeguards

The sponsors of the Third Workshop on Science and Modern Technology for Safeguards hope to promote improvements in international safeguards through the incorporation and use of results from science and advanced technology development. The workshop will be held November 13–16, 2000, in Tokyo, Japan. The Japan and Korea chapters of INMM and the Australian Safeguards and Nonproliferation Office are hosting this three-day event.

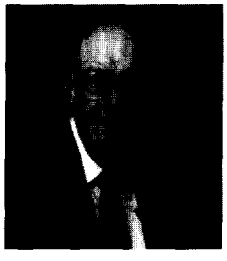
The Institute of Nuclear Materials Management and the European Safeguards Research and Development Association are cosponsoring this event. Their goal is to inform the safeguards community about current research in the natural and social sciences and selected, advanced technologies that could be used to support needed advances in international safeguards, and that will become available for use in the next few years. The two associations also want to stimulate the application of such science and advanced technology to safeguards by providing an opportunity for technical interchange between researchers and safeguards experts.

The third workshop will have four working groups that will consider the topics of:

- regional systems and state systems of accounting and control
- social-political aspects of safeguards
- safeguards challenges of future energy technologies, and
- automation, robotics, and expert software.

The registration fee for the workshop is $125. Registration materials will be available after Aug. 1, 2000, from INMM Headquarters or on the INMM Web site at http://www.inmm.org. For more information, contact INMM Headquarters at 60 Revere Drive, Suite 500, Northbrook, IL 60062 U.S.A. For more information call 847/480-9573, fax INMM at 847/480-9282, or E-mail inmm@inmm.org.

In Memoriam
Louis W. Doher (1922-2000)



The INMM lost a valued member with the death of Louis W. Doher on February 25, 2000. Mr. Doher joined the INMM in October 1960.

He began his employment in the nuclear field in April 1952 when he began work at Rocky Flats. When he retired on December 31, 1980, he was the manager of the chemistry standards laboratory where he was responsible for providing calibration services for production support, research, and accountability projects. Mr. Doher received a bachelor of science degree in pharmacy and a master of science degree in pharmaceutical chemistry from the University of Colorado. In addition to INMM, he was a member of the American Chemical Society and the American Pharmaceutical Society.

Mr. Doher received the INMM Meritorious Service Award in 1976 for exceptional work and achievements with the N-15 Committee of the American National Standards Institute for which the INMM serves as Secretariat. In this capacity, he developed standards for the calibration of mass, volume, nondestructive assay, and nuclear calorimetry measurements. He implemented many of these standards at Rocky Flats.

Mr. Doher received the INMM Distinguished Service Award in 1980 for outstanding contributions to the fields of nuclear materials management, safeguards, and nuclear energy. This included implementing many of the standards at Rocky Flats, several NRC licensees, the International Atomic Energy Agency, and the European Safeguards Research and Development Association. Mr. Doher published several papers at many INMM conferences on subjects such as innovative methods for preparing analytical control samples, nondestructive assay measurement control, sampling studies, reporting of control systems, and volume calibration of nuclear material process tankage.

Mr. Doher was known not only for his technical competence in standards development and calibration, but also for his lively wit, generosity, and determination. Even after retirement, he continued to act as consultant to several ANSI committees, to two committees of the American Society for Testing Materials, and to countless individuals involved in nuclear materials management who called upon him for counsel.

New Members

James J. Busse
U.S. Department of Energy
1000 Independence Ave., SW
Forrestal Bldg.
Washington, DC 20585
202/586-1700
Fax: 202/586-0936
E-mail: james.busse@hq.doe

Colin J. Carroll
Sonalysts, Inc.
P.O. Box 280
Waterford, CT 06385
860/442-4355
Fax: 860/442-5080
E-mail: ccarroll@sonalysts.com

Young-Myung Choi
NTC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-2138
E-mail: ymchoi@nanum.kaeri.re.kr

Sang-Tae Chung
TCNC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-2903
E-mail: stchung@nanum.kaeri.re.kr

Ernest L. Farrow
Hartford Steam Boiler Inspection & Insurance Co.
4616 Cloverdale Loop
Hixson, TN 37343
423/870-2769
E-mail: ernest_farrow@hsb.com

Melvin J. Feather
SAIC
20201 Century Blvd.
Suite 300
Germantown, MD 20874
301/353-0183
Fax: 301/428-0145
E-mail: melvin.j.feather.ii@saic.com

Lynn A. Foster
Los Alamos National Laboratory
P.O. Box 1663
MS E513
Los Alamos, NM 87545
505/665-8261
Fax: 505/665-6160
E-mail: laf@lanl.gov

Andrew J. Hamilton
IAEA
Wagramerstrasse 5
P.O. Box 100, Rm. A1943
Vienna, A-1400
Austria
E-mail: a.hamilton@iaea.org

George C. Jobson
GNB
250 Berryhill Road
Suite 500
Columbia, SC 29210
803/214-5878
Fax: 803/214-5804
E-mail: gjobson@nukem.com

Igor Khripunov
Center for International Trade & Security
University of Georgia
204 Baldwin Hall
Athens, GA 30602
706/542-2985
Fax: 706/542-2975
E-mail: igokhrip@arches.uga.edu

Ho-Dong Kim
KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-2349
Fax: 82-42-868-8824
E-mail: khd@nanum.kaeri.re.kr

Jong-Sook Kim
TCNC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-8326
E-mail: jskim3@nanum.kaeri.re.kr

Dale Lancaster
Nuclear Consultants.Com
320 South Corl Street
State College, PA 16801
814/231-5223
Fax: 814/231-0497
E-mail: dale@nuclearconsultants.com

Byung-Doo Lee
KAERI
Safeguards Department
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-2374
E-mail: bdlee@nanum.kaeri.re.kr

Jong-Uk Lee
TCNC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-8332
Fax: 82-42-861-8819
E-mail: julee@nanum.kaeri.re.kr

Andy T. Luksic
Pacific Northwest National Laboratory
P.O. Box 999
MSIN K8-41
Richland, WA 99352
509/372-4153
Fax: 509/372-4412
E-mail: luksic@pnl.gov

Margaret H. Manning
Jupiter Corporation
2730 University Blvd. West
Wheaton Plaza North Suite 900
Wheaton, MD 20902
202/586-5491
Fax: 202/586-0936
E-mail: m.manning@jupitercorp.com

David J. Mercer
Los Alamos National Laboratory
Group NIS-5, MS E540
Los Alamos, NM 87545
505/665-8561
Fax: 505/665-4433
E-mail: mercer@lanl.gov

Gyung-Sik Min
TCNC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-8726
E-mail: gsmin@nanum.kaeri.re.kr

Won Woo Na
TCNC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-2336
Fax: 82-42-861-8819
E-mail: wwna@nanum.kaeri.re.kr

Soo-Jin Park
TCNC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-8128
E-mail: sjpark@nanum.kaeri.re.kr

Teressa Reed
Lockheed Martin Energy Systems
1099 Commerce Park
Oak Ridge, TN 37830
865/241-9695
Fax: 865/574-3900
E-mail: itv@y12.doe.gov

Arne Van Roon
Alyn Corp.
16761 Hale Ave.
Irvine, CA 92606-5006
949/475-1525
Fax: 949/475-2359
E-mail: avr@alyn.com

Jonathan S. Shieh
Taipei Economic & Cultural Office
Praterstrasse 31/15 OG
Wien, A-1020
Austria
43-1-212-4720-78
Fax: 43-1-212-4720-90
E-mail: jonathan@teleweb.at

Young-Joon Shin
KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-8229
E-mail: nyjshin@nanum.kaeri.re.kr

Dong-Sup So
KAERI
Safeguards Department
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-2953
E-mail: dsso@nanum.kaeri.re.kr

Michael E. Stein
Sonalysts, Inc.
P.O. Box 280
Waterford, CT 06385
860/442-4355
Fax: 860/442-5080
E-mail: mestein@sonalysts.com

James E. Stewart, III
Los Alamos National Laboratory
P.O. Box 1663, MS E540
Los Alamos, NM 87545
505/667-2166
Fax: 505/665-4433
E-mail: jstewart@lanl.gov

Jim Tushingham
AEA Technology
220 Harwell Laboratory
Didcot, Oxfordshire OX11 0RA
United Kingdom
44-1235-434853
Fax: 44-1235-434543
E-mail: jim.tushingham@aeat.co.uk

Carl A. Whitaker
Northeast Utilities
P.O. Box 128, Bldg. 47514
Waterford, CT 06385
860/440-2167
Fax: 860/440-2172
E-mail: whitaca@nu.com

Jon B. Wolfsthal
Carnegie Endowment for Intl. Peace
1779 Massachusetts Ave., NW
Washington, DC 20036
202/939-2287
Fax: 202/483-1840
E-mail: jwolfsthal@ceip.org

Yeo-Chang Yoon
TCNC, KAERI
P.O. Box 105, Yusong
Taejon, 305-600
Korea
82-42-868-8334
E-mail: ycyoon@nanum.kaeri.re.kr

DOE Halts Incinerator Plans in Idaho

The U.S. Department of Energy agreed in late March to halt plans to build a plutonium waste incinerator at the Idaho National Engineering and Environmental Laboratory, about 100 miles west of Yellowstone National Park. The agreement was reached in settlement of a lawsuit filed against DOE by Keep Yellowstone Nuclear Free, a citizens' group.

The DOE will continue with the construction of a mixed-waste treatment facility at INEEL to process most of the site's existing stored transuranic waste and will pursue regulatory options that may make incineration of the small quantity of remaining material unnecessary. Energy Secretary Bill Richardson will also form a blue-ribbon panel to assess and recommend new technology alternatives to incineration.

Keep Yellowstone Nuclear Free claimed that incineration would release radioactive materials into the environment and cause damage to wildlife and people.

The DOE has an obligation to treat and remove 65,000 cubic meters of waste from the state of Idaho by 2018 in accordance with a settlement agreement signed with the state. DOE and the contractor of the waste treatment facility are requesting a partial permit that would allow them to begin construction on the other components of this facility.

The blue-ribbon panel will report its recommendations to Richardson in December 2000.

DOE Announces LLW and MLLW Treatment and Disposal Sites

In February, the U.S Department of Energy released its final decision for low-level waste and mixed low-level waste treatment and disposal sites. This enables the department to move forward with the closing of former defense nuclear facilities and to redirect the millions of dollars now being spent on waste storage back into cleanup work. The DOE's decision follows a December 10, 1999, Notice of Preferred Alternatives. The Record of Decision is consistent with those preferred alternatives.

The decision, the result of two years of study and discussion with affected parties, supports a continuation of many of the treatment and disposal activities already underway, relying for future disposal on sites that already have the capacity to handle low-level and mixed low-level waste.

For low-level waste treatment, the DOE will continue the practice of each site treating its own waste. For low-level waste disposal, DOE will continue disposal of onsite waste at sites that already have low-level waste disposal facilities, including Hanford, Idaho, Los Alamos, Nevada Test Site, Oak Ridge, and Savannah River. The department will continue to use the Hanford site and the Nevada Test Site for disposal of low-level waste from other DOE sites that don't have disposal capacity. For mixed low-level waste treatment, the DOE will continue to use Hanford, Idaho, and Oak Ridge to treat waste from other DOE sites, and will begin to use Savannah River to treat waste from other DOE sites. For mixed low-level waste disposal, the DOE will use the disposal facilities already constructed at the Hanford site and at the Nevada Test Site for off-site waste.

This decision is intended to improve safety and address public health concerns related to untreated waste now in storage at DOE sites around the country, according to the Department of Energy. The decision also will improve the efficiency and flexibility of operations, and decrease costs.

This Record of Decision was published in the Federal Register on February 25, 2000, and is posted at http://www.em.doe.gov under "Publications" and the "List of Publications" on the Internet. Copies of the Record of Decision are available by calling 800/736-3282. In the District of Columbia, call 202/863-5084.

IAEA Appoints Representative to United Nations

Kwaku Aning has been appointed as the representative of the director-general of the International Atomic Energy Agency to the United Nations and as director of its office at United Nations Headquarters in New York City. Aning assumed his duties on February 1, 2000.

Aning has held several posts at the United Nations in New York and the United Nations Conference on Trade and Development in Geneva since 1977. His assignments include serving as secretary of the organizational committee of the Administrative Committee on Coordination from 1998 to 2000 and serving as secretary of the U.N. Committee on Science and Technology for Development from 1995 to 1998). Aning was also regional coordinator for elections in Angola (U.N. Angola Verification Mission UNAVEM II) and deputy to the humanitarian assistance coordinator in Angola from 1992 to 1993. Aning was secretary of the Preparatory Committee of the U.N. Conference on Science and Technology for Development in 1978 and 1979 and he has also worked on several U.N. technical cooperation projects on technology policy issues, in particular information and communication technologies.

Aning obtained his doctorate degree in metallurgical engineering from Columbia University, his master's degree in solid state physics from Princeton University, and his bachelor's degree in mechanical engineering (summa cum laude) from the University for Science and Technology in Kumasi, Ghana.

Aning has edited two books on infor-

mation and communication technologies and published several articles in scientific and technical journals. A citizen of Ghana, Aning was born in 1946.

DOE Announces Actions to Improve Safety Management at Oak Ridge

A U.S. Department of Energy investigation of a December 1999 explosion at the Y-12 Plant in Oak Ridge, Tennessee, found that the accident could have been prevented if managers and workers had followed DOE guidelines for planning work and analyzing potential hazards consistent with the department's Integrated Safety Management program. The department also released a series of corrective actions it is taking to help prevent similar accidents in the future.

"This investigation shows that there were failures in the Energy Department's Oak Ridge Operations Office and at every level of the Lockheed Martin Energy Systems management chain," said Dr. David Michaels, DOE assistant secretary for environment, safety and health. "I am especially concerned that managers and workers failed to understand the nature of the chemical hazard involved, and failed to obtain the information or expertise needed to handle the unusual or unexpected conditions they faced," he said.

The accident took place on December 8, 1999, after Y-12 workers used a new procedure to change out the crucible in the caster furnace, an operation that last occurred in 1993. When workers removed a hose from the crucible, several gallons of chemical coolant — a sodium-potassium liquid metal alloy — sprayed into the furnace. Several days later, workers noticed unusual conditions in the furnace and sprayed mineral oil on the deposits to minimize oxidation. The chemical explosion occurred when workers then used metal probes to break up and remove the coolant spill. The explosion's damage was exacerbated by the lack of appropriate protective equipment for personnel. A total of 11 workers were injured; three required hospitalization.

The investigation concluded that the direct cause of the explosion was the impact of a metal tool on the shock-sensitive mixture of liquids. Warnings against such an action are contained in safety sheets and numerous publications and lessons learned documents, all available on site.

The report concluded that the primary cause of the accident was the site's multiple failures to effectively implement ISM practices. "Implementation of ISM was significantly deficient, indicating a lack of understanding of the policy, a failure to adhere to established procedures, and a continuing reliance on informal, expert-based approaches to work and hazard control," the report concludes.

In response to the investigation, the department's Oak Ridge Operations Office has put in place several corrective actions, which include:

- Improving communications and safety training for supervisors and workers
- Increasing worker involvement in safety planning and their involvement in the ISM program itself
- Revising procedures to specifically address operations such as the one that led to the explosion
- Clarifying start-up and shut down procedures in an emergency
- Conducting frequent, no-notice inspections by the Y-12 independent assessment team
- Increasing management presence on the work floor to obtain first-hand feedback from workers, and
- Training managers and supervisors in decision-making.

The investigation also showed that the Y-12 site's emergency medical responses were generally effective. The most severely injured were assisted promptly. The Y-12 fire department and radiation control personnel responded promptly and effectively to transport injured workers and prevent the spread of contamination.

Supercomputer Completes 1st 3-D Simulation of Weapons Trigger

In February, U.S. Secretary of Energy Bill Richardson announced that the U.S. Department of Energy's Stockpile Stewardship Program successfully completed the first-ever three-dimensional simulation of a nuclear weapon "primary" explosion using the IBM Blue Pacific supercomputer at the DOE's Lawrence Livermore National Laboratory.

The simulation required about 300,000 megabytes of RAM. A conventional computer is equipped with only a few hundred megabytes of RAM. Even with the supercomputer, the calculations ran for more than 20 days. A desktop computer would have taken 30 years to accomplish the same task.

The DOE joined with computer manufacturing companies to develop computers with unprecedented speed and capacity. Before ASCI supercomputers, none of the world's computers have been able to meet the speed required for the 3-D simulation, nor did they have the capacity to handle such complex calculations. It's now routine for DOE's Lawrence Livermore, Los Alamos, and Sandia national laboratories, with the help of U.S. computer industry partners IBM, SGI, Intel, and others, to do stockpile stewardship simulations that would have been impossible with previous computing capabilities.

Nine Countries Issue Statement on Generation IV Nuclear Power Systems

Nine countries issued a joint statement agreeing to pursue Generation IV nuclear power systems as a potential next generation option for the future.

Argentina, Brazil, Canada, France, Japan, South Africa, South Korea, the United Kingdom, and the United States released the joint statement in February.

Generation IV nuclear power systems represent economically competitive, advanced nuclear reactor technology to be deployed in the next 20 years, when demand for electricity worldwide is expected to increase dramatically.

The statement was released following a workshop held in Crystal City, Virginia, U.S.A., on January 27–28, 2000, where government officials discussed the attributes of next generation nuclear reactor technology. In addition to the attending countries, the workshop was attended by representatives of the International Atomic Energy Agency, the OECD Nuclear Energy Agency, the U.S. State Department, the American Nuclear Society, and the U.S. Department of Energy's Nuclear Energy Research Advisory Committee.

New Manufacturing Plant Opens

A new manufacturing plant that will produce a canister system for the storage and transport of spent nuclear fuel opened in March in Canonsburg, Pennsylvania. The facility is owned by Ionics, Inc.

The new facility will enable Ionics' fabricated products division to maintain its position as a quality-oriented custom alloy steel fabrication center. The refurbished heavy industrial manufacturing plant will add to the existing capacity of Ionics' plant in Bridgeville, Pennsylvania.

Last October, Ionics announced that it had received an award for the $10 million first phase of a multi-year contract from NAC International to manufacture a Universal Multi-Purpose Canister System® for the storage and transportation of spent fuel.

Institute to Host PATRAM 2001

The Institute of Nuclear Materials Management will host the 13th International Symposium on the Packaging and Transportation of Radioactive Material in Chicago, Sept. 3–7, 2001, at the Chicago Hilton and Towers.

The PATRAM symposia are held every three years and dates from the early 1960s. It brings government and industry leaders together to share information on innovations, developments, and lessons learned about radioactive material packaging and transportation. PATRAM is sponsored by the U.S. Department of Energy, in cooperation with the International Atomic Energy Agency.

Author Submission Guidelines

The *Journal of Nuclear Materials Management* is the official journal of the Institute of Nuclear Materials Management. It is a peer-reviewed, multidisciplinary journal that publishes articles on new developments, innovations, and trends in safeguards and management of nuclear materials. Specific areas of interest include physical protection, material control and accounting, waste management, transportation, nuclear nonproliferation/international safeguards, and arms control and verification. *JNMM* also publishes book reviews, letters to the editor, and editorials.

Submission of Manuscripts: *JNMM* reviews papers for publication with the understanding that the work was not previously published and is not being reviewed for publication elsewhere. Papers may be of any length.

Papers should be submitted in *triplicate*, **including a copy on computer diskette**. Files should be sent as Word or ASCII text files only. Graphic elements must be sent in TIFF format in separate electronic files. Submissions should be directed to:

Dennis Mangan
Technical Editor
Journal of Nuclear Materials Management
60 Revere Drive, Suite 500
Northbrook, IL 60062 USA

Papers are acknowledged upon receipt and are submitted promptly for review and evaluation. Generally, the author(s) is notified within 60 days of submission of the original paper whether the paper is accepted, rejected, or subject to revision.

Format: All papers must include:

- Author(s)' complete name, telephone and fax numbers and E-mail address
- Name and address of the organization where the work was performed
- Abstract
- Camera-ready tables, figures, and photographs in TIFF format only
- Numbered references in the following format:
  1. F.T. Jones and L.K. Chang, "Article Title," *Journal* 47(No. 2):112–118 (1980).
  2. F.T. Jones, *Title of Book*, New York: McMillan Publishing, 1976, *pp.* 112–118.
- Author(s) biography

Peer Review: Each paper is reviewed by two or more associate editors. Papers are evaluated according to their relevance and significance to nuclear materials safeguards, degree to which they advance knowledge, quality of presentation, soundness of methodology, and appropriateness of conclusions.

Author Review: Accepted manuscripts become the permanent property of INMM and may not be published elsewhere without permission from the managing editor. Authors are responsible for all statements made in their work.

Reprints: Reprints may be ordered at the request and expense of the author. Order forms are available from the Institute's office, 847/480-9573.

Chapters

continued from page 6

- Yuri Volodin, Gosatomnadzor of Russia — Chair
- Alexander Izmailov, Eleron, Minatom of Russia — Vice Chair
- Andrew Zobov, Karnegi Fund, Moscow Branch — Secretary

Most of activities of the Russian Federation Chapter focused on the participation of members in the large, comprehensive projects of physical protection upgrading at a number of Russian nuclear facilities. Other important activities include working on the computerization of nuclear material accountability and control; creation of the state system for accounting and control; development of the state system for the MPC&A oversight; and strengthening the technical capabilities of strategic nuclear material transportation and protection.

Yuri Volodin
Chair
INMM Russian Federation Chapter
Gosatomnadzor of Russia
Moscow, Russia

Southwest Regional Chapter

The Southwest Regional Chapter held elections for executive committee positions in November 1999. The positions of chapter president, vice president, secretary/treasurer, and for two members-at-large were open for selection by the membership. The newly elected officials are:

- Chad Olinger, Los Alamos National Laboratory, NIS-7 — President
- Cary Crawford, Wackenhut Services, Inc., NNSI/CTA — Vice President
- Lawrence Kwei, US Department of Energy/RFFO — Secretary/Treasurer
- Wendy Doyle, Aquila Technologies Group, Inc. and Donnie Glidewell, Sandia National Laboratory — Members-at-Large

The Southwest Chapter's top priority for this year is to strengthen communication with members. To this end, the chapter has developed a membership chairperson position, which will be responsible for membership development and will oversee maintenance of the chapter membership database. The chapter has also established state coordinators to enhance chapter activities on a statewide level. Further, the chapter is exploring the possibility of developing and maintaining a chapter Web site to provide updates to the membership.

The chapter is beginning planning for an annual meeting. Because of the limited availability of travel funds for federal and federal contractor employees, the chapter is exploring the potential for presentation of the annual meeting via interactive television technology. This technology is increasingly being used by the Department of Energy for working group and quality panel meetings. The chapter is currently looking at a date in early May for meeting.

Lawrence Kwei
Secretary/Treasurer
Southwest Chapter, INMM

ADVERTISER INDEX

Performance Validation of Monitoring Systems for Strengthened Safeguards

Rodney Martin
National Security Division,
Pacific Northwest National Laboratory

Abstract

International Atomic Energy Agency safeguards have traditionally relied on material balance accounting at declared facilities within a country. However, as the Agency moves to apply integrated safeguards concepts on a country-wide basis to detect clandestine nuclear material activities in both declared and undeclared facilities, new tools are needed to permit the Agency to satisfy safeguards objectives within imposed resource and cost constraints. If properly implemented, remote and unattended monitoring can provide assurance that materials are not diverted and that the safeguards system is functioning as required and is producing valid results.

A concept for developing monitoring systems that provide assurance of proper system performance is described here. The approach is based on evaluation of the sequential pattern of operations and data relationships, and implementation of a system of measurements and tests to validate operational performance. A key feature is the analysis of information and data from the monitoring system for use by an off-site inspectorate. Example applications of the generic concepts to a measurement system and to reprocessing operations are provided.

Introduction

IAEA safeguards have traditionally focused on detecting the diversion of nuclear materials from declared facilities. Agency safeguards have relied on special nuclear material accountancy, with periodic measured physical inventories to draw a material balance around a declared nuclear facility. The material balance is compared to statistical control limits based on propagating measurement uncertainties and evaluated to detect the loss of a significant quantity of material.

In the 1990s, the Agency embarked on a program to develop new safeguards techniques to detect undeclared nuclear activities and to improve cost-effectiveness. The integrated system, resulting from a combination of traditional and strengthened safeguards elements, focuses on a countrywide analysis of a wide range of information to detect undeclared nuclear material and activities at declared facilities and elsewhere.

A key component of strengthening measures is the introduction of advanced technology and the management of information and data to increase safeguards effectiveness and efficiency at declared facilities. This approach is generally based on acceptance by the IAEA of safeguards data derived from the use of host-provided equipment. This paper describes concepts that can be used to increase assurance that materials are not being diverted and that the analysis of the system data and relationships indicates that the safeguards system is functioning correctly and is producing valid results. These same concepts can also provide a quality assurance function for the state system of accounting and control.

Strengthened Safeguards

One of the best techniques for the control of nuclear materials is continuous monitoring of material flows and process operations. In this concept, data from a series of acquisition devices is used to verify nuclear material presence, assure nuclear material flows only via approved pathways, assess whether monitoring/measurement instrumentation is functioning correctly, and provide timely detection of anomalies which may indicate the loss or diversion of material. An advantage of this system is the timely detection, evaluation, and resolution of process variation; e.g., inadvertent process actions, records, and reporting errors. These nonstandard variations may impact the ability of the material accountability system to detect the loss of material or may be difficult to resolve when not detected until the end of a material balance period. Alternatively, the monitoring of process data as a function of time and comparison with the normal or expected result make this a powerful tool for surveillance of plant operations and the performance of the safeguards system. Many of the sources of data will be correlated through time and analysis of these combinations of data can also be used to detect anomalies. The acquisition and analysis of large quantities of data in real time and the complexity of the data relationships make it much more difficult to spoof the monitoring system.

Remote monitoring can be used to implement safeguards more efficiently. Monitoring has been used in a number of storage applications for surveillance of reprocessing operations and for tracking spent fuel transfers from a basin into long-term dry storage. One of the factors necessary to use remote monitoring

for achieving safeguards objectives is the assurance that the remote monitoring system has not been compromised so as to create a false record of events. Confidence in system performance can be obtained by conducting inventories and inspections. However, it is also possible to acquire and analyze information created by the monitored process to obtain increased confidence in the performance of the remote monitoring system.

Measures can be developed to provide a high level of assurance regarding system performance through analysis of time-sequenced information. To establish a high-assurance monitoring system, a detailed analysis is conducted of the sequential events that occur in the monitored process. Based on this analysis, data and information characteristic of each step in the process are identified and techniques are developed to acquire and analyze this sequential data. In developing these techniques, efforts are made to identify data that indicates normal process operations as well as to flag data that indicates abnormal or anomalous conditions. Attempts are also made to incorporate duplicative and correlated indicators of normal process operations, which adds to the complexity of trying to spoof the process monitoring system. The monitoring system is essentially based on development of a quality assurance function for the normal process operations and performance of a vulnerability analysis to detect anomalies and abnormal situations.

The data acquisition devices are a critical part of the monitoring system. However, there is another essential component in an effectively designed monitoring system. This component deals with the acquisition and analysis of the mountains of data generated by the process monitoring devices. The software used in the analysis of this information plays a key role in ensuring the reliability of the information and in analysis and presentation of the accumulated data in a format for review and evaluation by an inspector. The approach is to process raw data documenting each processing step and to create an auditable trail. Statistical or other techniques are applied to assess the probable validity of each data point in the data stream. Adaptive modeling may be applied when correlations should be present in the data field. Depending on the particular type of process information acquired, it may be desirable to have the information retrievable in the form of tables, graphs, calculations, or summary conclusions designed to aid the inspector in reaching safeguards conclusions. This approach for process monitoring is best illustrated by examples as discussed in the following sections.

Monitoring Measurement Systems

Most people think of remote monitoring as it applies to containment/surveillance systems in storage areas. However, these same concepts can be applied to a variety of other applications, including monitoring of measurement systems and processing operations. There are currently a number of potential applications for measurement of plutonium materials excess to weapons programs that involve measurement of isotopic ratios using a Ge(Li) gamma-ray spectroscopy system and measurement of plutonium mass using a neutron multiplicity counter. Techniques using this equipment are being developed for measurement of plutonium in both classified and unclassified forms. While valid techniques exist for assessing performance of an unclassified system by a hands-on inspectorate, the use of unattended or remote monitoring techniques, or measurement of classified materials with an information barrier, creates additional challenges for validating measurement system performance.

IAEA inspections are currently conducted on plutonium oxide no longer required for defense purposes in the U.S. at Rocky Flats and Hanford under the Voluntary Offer Safeguards Agreement. These and other plutonium materials at these two locations were scheduled for stabilization and repackaging into U.S. Department of Energy standard 3013 containers beginning in 1999. Plans call for all of the materials from both locations to be subsequently transferred to the Savannah River Site for long-term storage. These materials will be placed under IAEA verification measures with the goal of ensuring irreversible removal of these materials from nuclear weapons programs. The intent is for the IAEA to monitor these materials under the Trilateral Initiative; however, because trilateral legal arrangements have not been finalized, these materials may initially be placed under IAEA inspection through the VOA.

Beginning in January 2000, Rocky Flats was scheduled to begin transferring stabilized plutonium materials to Savannah River in 9975-type shipping containers that will be placed into storage in the K-Reactor Area material storage. Initial shipments from Rocky Flats will consist of plutonium metal followed by oxide materials currently under IAEA safeguards. Shipping containers cannot be opened in KAMS so the 9975-type containers will be subjected to receiver's verification, placed on pallets and sealed with radio frequency tags, and stored in identified KAMS locations under closed-circuit television surveillance. Receiver's measurements on the 9975-type containers will be performed using a Ge(Li) isotopic measurement system and a neutron multiplicity counter. These measurement devices will be jointly used by the facility and the IAEA and the output from these nondestructive assay instruments will be split to separate facility and IAEA shift registers and computers.

A variety of actions are necessary to authenticate the performance of these measurement systems and the application of containment and surveillance through the measurement-to-storage process. However, in this article, attention will be focused only on the measurement process. The basic process should consist of the following actions whether performed under an unattended or a remote monitoring regime:

- Secondary measurement standards may be created at Rocky Flats based on calorimetric measurement of stabilized materials in DOE standard 3013 containers. The plutonium values on these materials would be validated by the IAEA. A series of measurements of these standards should be performed initially to qualify the measurement system, and the standards should be measured on a periodic basis thereafter to assure continued unbiased measurement performance.

- Control standards should be created and measured dur-

ing each measurement period to ensure that measurement instruments are functioning properly. The controls do not necessarily have to be representative standards; e.g., a ^{252}Cf source might be used as a control for the NMC. Controls might be measured before and after daily counts, and perhaps at random periods during the day, depending on count times, number of items, etc.

- The IAEA should evaluate control and standards data through time, and on a comparative basis. The statistical analysis of this data can be automated and provides increased assurance of measurement system performance.

IAEA authentication of the measurement instruments and software, and validation of the mass and isotopic values of the standards, provides some assurance of measurement results. However, a variety of other techniques can be used to authenticate and increase confidence in measurement system performance. Most of these techniques can be used in an unattended or remote monitoring mode, and many can be considered for use during measurement of classified materials.

Time Interval Analyses

Statistical tests can be performed on data generated at different time periods during the measurement. The simplest option is to perform a Chi-square test between data from different time periods. The test should determine whether the differences are within statistical variations. Another check would be to test the statistical quality of the data as the measurement proceeds, showing that results continue to improve through each time interval.

A number of ratio techniques can be used to monitor system performance. These include evaluation of isotopic ratios based on a variety of peaks in the spectrum and determining the consistency of these ratios as a function of energy. Other techniques could compare background peak ratios between measurements, consistency between "like" containers (neutron count rates, gamma ray intensities), ratios of full energy to escape peaks, etc. Consideration might also be given to doing peak shape analysis and performing consistency checks within and between measurement spectra.

Adding a Source

For a variety of techniques applicable to these systems, adding a source may aid system validation. For example, adding a ^{252}Cf source to a NMC count may produce a negative alpha and lead to rejection of that measurement result if this test is performed as a validation criteria. Addition of a ^{137}Cs source above a predefined source strength to the Ge(Li) gamma-ray isotopic system will cause that system to provide results of "excessive Chi-square" or "Analysis failed: Fit results failed to converge." Use of these techniques can indicate that the system is functioning, is performing programmed analysis of the data, and is providing appropriate results. Random insertion of this option could provide increased assurance of correct system performance. Another option would be to add a source during only a portion of the measurement cycle and have software look for differences between timed segments. This would again provide data indicative of a functioning measurement system. A variant of this technique for the gamma-ray isotopic system would be to also analyze a background peak in every spectrum and to perform analyses on this result through time. An option to adding a source would be to add a moderator or a neutron absorber during a NMC measurement. Again, this could be structured to check for consistency in the singles, doubles, and triples observed under varying conditions.

While instrument authentication and measurement of standards provide a measure of system validation, the addition of the types of data analysis just described can significantly increase confidence in system performance. It should be noted that a number of these techniques involve only the addition of software to perform analyses and comparisons between different time sequences. Assuming multiple analyses of this type are interspersed within the measurement cycles, it becomes much more difficult to successfully defeat the monitoring system without detection. This is because false records must be created for each of the tests performed which are consistent with the data acquired within and between measurements. The addition of these system-assurance checks does add a requirement for software to provide quality assurance for the data and information, to check for logical consistency and relational data patterns, and to organize and analyze the large amounts of data created. This means that a significant amount of data and associated information must be assessed for quality, processed, and presented for evaluation by an inspector. However, properly configured software should transform the raw data into more useful information for assessment. In this way, an inspector may perform an analysis only to detect anomalies, just spot check the data, and confirm that the analyses were correctly performed. Further system checks and validation could be implemented as part of the annual physical inventory verifications, short-notice inspections, or event-driven inspections.

Other techniques can be applied to measurement systems. Using what are referred to as "collaboratory" concepts, it is possible to develop an Internet-aware instrument control platform that will allow a remote user to run analytical instruments, access and analyze data, and perform system checks remotely. These concepts can be used for unattended remote monitoring or to perform random inspections of measurement performance on a real-time basis. System validation techniques may also play a significant role in wide-area environmental monitoring. In this case, monitoring plays a role in ascertaining whether the sampler is functioning as required, in ensuring the quality of the system, and in organizing the samples and associated information.

Monitoring Processing Operations

Remote monitoring concepts can also be applied to processing operations. Again, the same process is applied; i.e., an analysis is performed of the sequential flow of materials through the process

and information is collected to confirm consistency with expected operations. In this case, a surveillance system using monitoring techniques is implemented through the entire process. Activities that are subject to monitoring for a reprocessing plant include:

- **Accountability Measurements.** Process solution bulk measurements can be performed to determine high-precision tank solution levels and densities. Accountability results are obtained by multiplying the solution bulk quantity by the SNM concentration derived from analysis of samples or NDA. Monitoring the measurement process can confirm solution volumes and provide tank densities for comparison with densities of samples pulled for analytical measurements. In addition, monitoring can confirm that appropriate mixing of tank contents occurred prior to sampling (note that density comparisons also support this conclusion), that the correct tank was sampled, and that the correct number of samples was taken.

- **Transfer Monitoring.** Transfer monitoring tracks the movement of nuclear material solutions within the process. Before and during a transfer, sensors can monitor that the sequence of valves open corresponds to that expected for an approved transfer between two parts of the process in accordance with established procedures. Additionally, monitoring of the status of other closed valves indicates that alternate transfer routes are blocked. Transfer monitoring may be activated by the start/stop of a transfer pump, steam jet, or airlift. It can be followed by observing changes in levels (comparison of volumes removed to quantity gained) for the tank(s) involved, and may be verified by temperature changes and/or flows in transfer piping.

- **Diversion Monitoring.** Sensors can also be deployed within a process to detect diversion of material. Devices may be used to detect liquid in lines that should be empty, and monitoring may be employed to detect SNM in streams that should not contain these materials and/or should contain only low levels of SNM. A variety of C/S devices can be employed to ensure that no unauthorized access to plant processes and equipment has occurred. Of course, one of the best techniques is simply to monitor tank levels of static inventory solutions through time.

Techniques that have been used successfully for analysis of this type of information include listing devices in a table and noting any activity. Focusing only on devices activated during a period concentrates attention on process areas where changes have occurred. In this way, the process changes can be evaluated, usually by looking at graphical representations, to see if the activities were conducted in accordance with established procedures. These evaluations provide significant benefits in timeliness and cost reduction.

Conclusions

Remote monitoring of processes can play an important role in implementing safeguards more efficiently. The acquisition and analysis of data and information on a real-time basis can be used to track and monitor process operations, to verify compliance, and to detect anomalous conditions requiring further investigation. In most cases, monitoring relies on accumulation of easily acquired data and information related to the sequential conduct of the monitored process. It is the acquisition, organization, analysis, and presentation of the data and information in a form that lends itself to analysis and interpretation that forms the basis for use of this tool in achieving safeguards objectives.

It has been shown that monitoring can validate system performance and provide assurance that operations were conducted in accordance with established procedures. Proper development of the monitoring system using vulnerability assessments and consistency logic can produce a high-confidence safeguards tool. However, this must be combined with software that can transform large quantities of process data and records in real time into a form for interpretation, understanding, and decision making.

The reliability of data transmission is clearly another important consideration in developing the remote monitoring system. Visual representation of data, clustering of data sets, development of models, and identification of patterns are all tools that have been used in the analysis of these type of databases. While this methodology relies on an initial investment for data acquisition and transmittal devices, and for development of analysis software, after implementation it provides for much more effective use of resources and for more timely detection of anomalies. The high confidence that can be obtained through effective use of remote monitoring data should support the use of this cost-effective approach to provide assurance of non-diversion and to support a reduction in the frequency of routine inspections.

Rodney Martin is the International Safeguards Program manager at Pacific Northwest National Laboratory. For the four-year period before he transferred to Pacific Northwest in 1996, Martin served as the director/deputy director of New Brunswick Laboratory, the U.S. government's measurements and standards laboratory. Starting in 1975, Martin spent 17 years in the Department of Energy's Idaho field office, primarily as the safeguards branch chief responsible for MC&A and materials management programs, and later as director/deputy director of the safeguards and security division. His early career involved design and development of NDA systems for waste/scrap assay and nuclear material accountability at DOE's Rocky Flats plant.

A Simple Evaluation Model on the Effectiveness of Integrated Safeguards Implementation

Hiroshi Matsuoka
Japan Atomic Energy Research Institute
Tokyo, Japan

Note: The views expressed in this paper are the author's personal views and do not necessarily represent the views of the organizations with which the author is affiliated.

Introduction

Many countries concluding comprehensive safeguards agreements (INFCIRC/153 type) with the International Atomic Energy Agency are currently going to agree to a new additional protocol, INFCIRC/540. The protocol will make them provide more information to the IAEA. The expanded framework is expected to establish a stronger and more efficient IAEA safeguards system, which we call integrated safeguards. However, there seems to be no logical fundamentals that enable the inspectorate to derive a final evaluation from the information collected through the integrated safeguards implementation. In this paper, the author tries to make the fundamentals clear and proposes a simple practical model to evaluate the effectiveness of integrated safeguards implementation. In addition, this model is shown to be useful for planning to improve the efficiency.

Index of the Effectiveness of Safeguards Implementation

The objective of the comprehensive safeguards is described in the INFCIRC/153. Evaluation of the safeguards effectiveness should be to estimate a degree of assurance how the objective is attained. In other words, we have to show the truth value of the proposition: "Any nuclear material in a state is not used for the manufacture of nuclear explosive devices."

This paper will give a simple model to calculate the "truth value" of nonmanufacture of nuclear explosive devices. Regarding the calculation, note that the truth value can be equal to any numerical value from 0 (= completely false) to 1 (= completely true). In this sense, fuzzy logic is applied.

Proliferation Activity and Its Steps

Proliferation activity to manufacture nuclear explosive devices needs many steps. One of the examples of the steps is "Operation of equipment for the uranium enrichment." Figure 1 shows all the steps composing proliferation activities. In the figure, we use the following categorization of nuclear material to simplify the following discussions:

- HEU: Highly enriched uranium directly used for nuclear explosive devices
- LEU: Uranium suitable for isotopic enrichment excluding HEU
- PU: Plutonium or uranium-233 directly used for nuclear explosive devices
- SF: Irradiated nuclear fuel containing PU
- FF: Unirradiated nuclear material suitable for fuel fabrication to produce SF

It is useful to note that the structure of steps combination consists of only two types as shown in Figure 2. "Production" of X needs both "operation" of the equipment to produce X and "acquisition" of the feed nuclear material X' for the production. This relation can be depicted as follows:

P(X) = O (process to produce X) and A (feed material X')
(1)

On the other hand, "acquisition" of X can be attained by implementing at least one step from the three: D(X), T(X) or P(X). This relation can be depicted as follows:

A(X) = D(X) or T(X) or P(X)
(2)

Regarding the above equation, note that "Acquisition of nuclear material from undeclared initial inventory" does not appear. It can be regarded as a part of T(X) or P(X) in the past before the starting point of safeguards agreement.

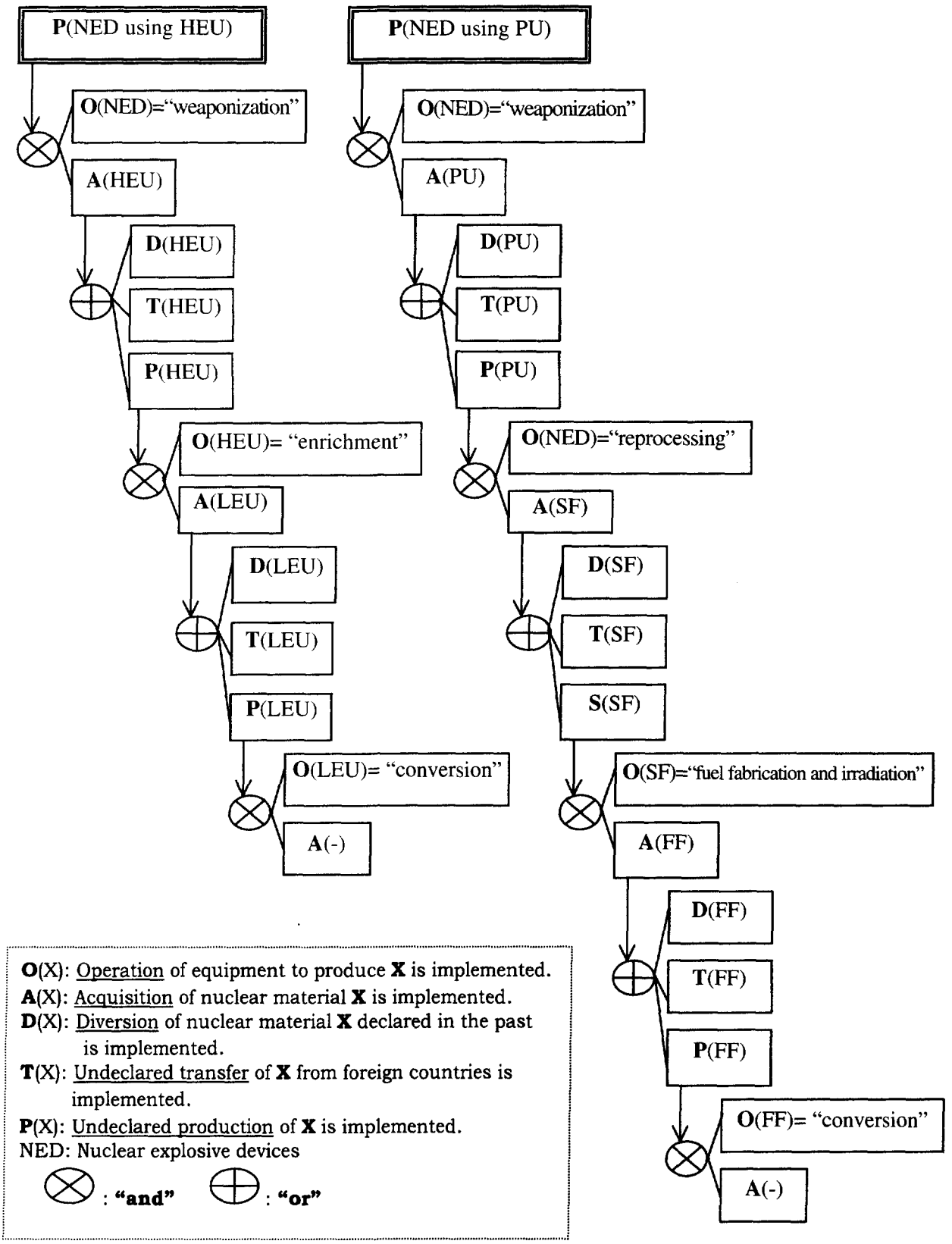


Figure 1. Proliferation activity and its steps

Proposal of a Simple Evaluation Model on the Effectiveness of Safeguards Implementation

Basic idea of considering the evaluation procedure

If any step depicted in Figure 1 is implemented, some indications will arise. Well-planned safeguards implementation will detect them. The relation is summarized in the following inference rules:

NED Manufacture → Step Implementation → Indication Detection

On the other hand, our objective is to calculate the truth value of nonmanufacture of NED, which is the negation of NED manufacture. Accordingly, it is a solution to consider the contraposition of the above inference rules. That is:

Non-detection of Indications → Non-implementation of Steps → Non-manufacture of NED

Along this order, we will discuss the calculation process of truth values.

Truth Values of the Propositions: "Nondetection of Indications"

At the beginning, we assume the following definition for the logical operation of negation:

(Truth value of Negative proposition) = 1 – (Truth value of the original proposition)
(3)

Under the above definition, a truth value 0.5 means neutral judgement because truth value of the Negative proposition is equal to truth value of the original proposition.

The first thing to be done is the determination of truth values of the following proposition:

- Kj: "Indication analysis by the inspectorate shows Step j was implemented."
  (4)

- ~Kj: "Indication analysis by the inspectorate shows Step j was not implemented."
  (5)

Here, j = D(X), T(X) or O(X), and X = HU, LU, PU, SF or FF.

Needless to say, a truth value of the above proposition Equation 4 or Equation 5 can be derived from the truth value of the other using Equation 3. This value should be determined by inspectorate according to the result of indication analysis regarding Step j.

Indication analysis assumed here is as follows:

Indication analysis on Step D: Analysis of MUF (Inventory difference)

Indication analysis on Step T: Analysis of international S/RD (Shipper/receiver difference)

Indication analysis on Step O: Analysis of information that may indicate undeclared process operation. In this analysis, the "physical model" developed by the IAEA will be very useful.

Truth Values of the Propositions: "Nonimplementation of Steps"

The second thing to be done is the determination of truth values of the following propositions:

- ~D(X): "Diversion of nuclear material X declared in the past is not implemented."
- ~T(X): "Undeclared transfer of X from foreign countries is not implemented."
- ~O(X): "Operation of equipment to produce X is not implemented."

Here, X = HEU, LEU, PU, SF or FF.

We need inference rules to derive the truth values of ~D(X), ~T(X) and ~O(X) from the truth values of Kj. [j = D(X), T(X) or O(X)]

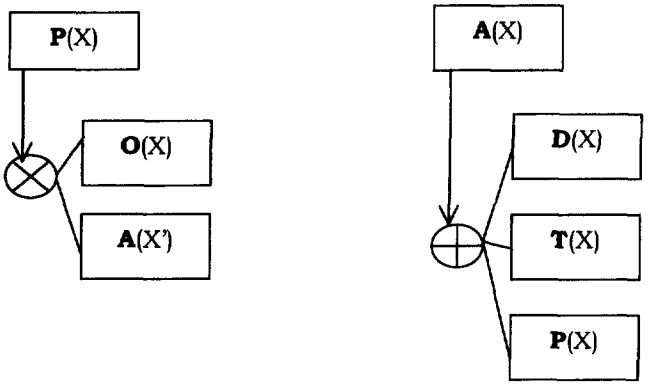


Figure 2. Structure of steps combination

Before considering the above inference rules, we will discuss the inference rules: D(X) → KD(X), T(X) → KT(X) and O(X) → KO(X). Generally speaking, the truth values of these inference rules are not 1. The reason is that inspectorate cannot always detect the indications arising from the implementation of steps. So, we define a parameter Rj:

Rj = {Truth value of Inference rule: "Step-j Implementation → Indication-j Detection"}
(6)

Considering the meaning of Rj, we can regard it as the multiplication of the following three possibilities:

- That indication arising from the implementation of Step j is correctly propagated into the information sources available for inspectorate
- That the inspectorate selects the information source as the target of indication analysis
- That the inspectorate can detect the indication through the indication analysis avoiding the confusion caused by the included information-noise (false information, measurement error and so on).

Consider some examples. In the case that j = D(X), the value

of Rj will become large when continuity of knowledge on the nuclear material flow is confirmed by analyzing domestic S/RD, containment/surveillance, item identification, and so on. In the case that j = T(X), the value of Rj will become large when no illegal trafficking is found in the survey of relevant information sources. In the case that j = O(X), the value of Rj will become large when the state has highly-opened information systems to the public. In the case that the inspectorate does not implement indication-j-detecting activities, then Rj = 0.

Coming back to the consideration on inference rules, we assume that the truth value of a contraposition of any proposition is equal to the truth value of the original proposition. As the result,

{Truth values of the inference rules: $\sim KD(X) \rightarrow \sim D(X)$, $\sim KT(X) \rightarrow \sim T(X)$ and $\sim KO(X) \rightarrow \sim O(X)$} = Rj
(7)

Here, j = D(X), T(X) or O(X), respectively, and X = HEU, LEU, PU, SF or FF.

Next, we assume the following definition for our deduction principle.

(Truth value of Conclusion) = 0.5 + (Truth value of Inference Rule) × {(Truth value of Assumption) – 0.5}
(8)

This definition means that deviation from the neutral judgment propagates from assumption to conclusion in proportion to the reliability of inference rule.

Lastly, we can calculate the truth values of ~D(X), ~T(X) and ~O(X) from Kj (= the truth values of Kj) by using Equations 3, 6, 7 and 8. Thus, the following equations are obtained:

{Truth value of ~D(X)} = 0.5 + RD(X) × {0.5 - KD(X)}
(9)

{Truth value of ~T(X)} = 0.5 + RT(X) × {0.5 - KT(X)}
(10)

{Truth value of ~O(X)} = 0.5 + RO(X) × {0.5 - KO(X)}
(11)

Truth values of the propositions: "Nonmanufacture of NED"

At this stage, we need rules to derive a truth value of ~P(NED using HEU) or ~P(NED using PU) from the truth values of ~D(X), ~T(X) and ~O(X). For this purpose, we assume the following two special definitions only used for the evaluation discussed here:

[Truth value of ~P(X)] = Maximum {[Truth value of ~O(X)], [Truth value of ~A(X')]}
(12)

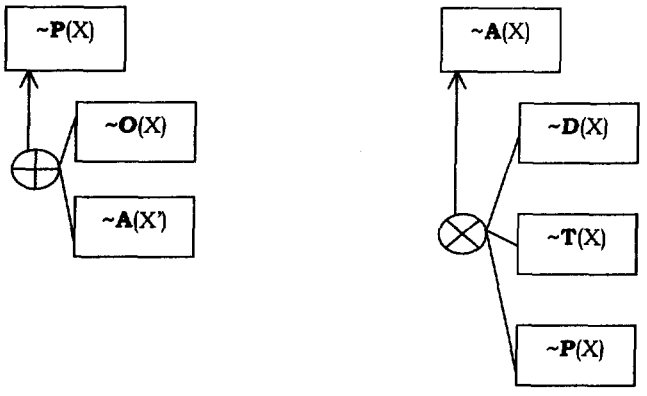


Figure 3. Numerical simulation on U-235 route

[Truth value of ~A(X)] = 0.5 + 0.6 × {[Truth value of ~D(X)] - 0.5}
+ 0.2 × {[Truth value of ~T(X)] - 0.5}
+ 0.2 × {[Truth value of ~P(X)] - 0.5}
(13)

The first definition (Equation 12) means that assurance-degree of nonproduction is given by the maximum value between the assurance-degree of nonoperation of production equipment and the assurance-degree of acquisition of feed material.

The second definition (Equation 13) means that deviation of assurance-degree of nonacquisition of nuclear material from the neutral judgement is given by the weighted summation of deviations from the neutral judgement of nondiversion, non-transfer from the foreign countries, and non-production. The weight values of them are 0.6, 0.2, and 0.2, respectively. It is, of course, possible to assume the other values.

Now, we can come back to the proposition: ~P(NED using HEU) or ~P(NED using PU) by repeating the elemental routes shown in Figure 3 by using Equations 12 and 13.

Numerical Simulations

Figure 4 shows the case studies of numerical simulations regarding the evaluation of non-manufacture of nuclear explosive devices using HEU.

We calculate the truth value of the proposition ~P(NED using HEU) when no indication is found through the indication-detecting activities. Assumptions of the numerical values of Kj and Rj are also shown in Figure 4. Equations used here are Equations 9, 10, 11, 12 and 13.

From the case studies, the truth value of the proposition ~P(NED using HEU) is calculated as 0.848 in case of the conventional safeguards implementation. This value will be improved up to Max{0.84+0.1Q, 0.908} by the integrated safeguards Implementation. This result shows the effectiveness of Integrated Safeguards. Here, Q is a parameter defined by Rj when j = O(HEU) = "enrichment." That is, Q means a detection possibility of enrichment process operation.

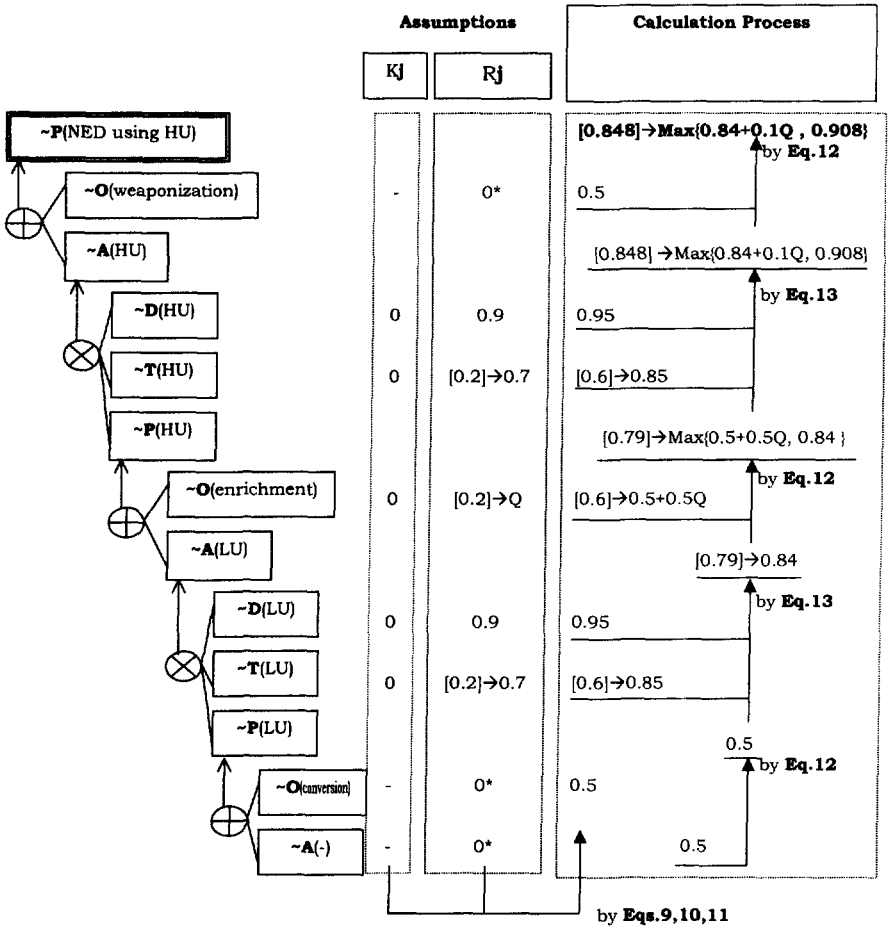
Roughly speaking, in the case of a highly information-opened country, the value of Q will be larger. If Q becomes larger than 0.68, Truth value of ~P(NED using HEU)} is given by 0.84+0.1Q and does not depend on the truth value of ~A(LEU) or ~D(LEU). This means that conventional safeguards implementation to confirm ~D(LEU) can be reduced for such country without decreasing the effectiveness. This result shows that well-planned safeguards implementation can attain higher efficiency.

In the above simulation, the values of Kj and Rj (j= D(X), T(X) or O(X)) are initially given. However, these values should be determined according to the results of safeguards activities. In this regard, some criteria will be needed at the implementation phase.

Conclusion

One of the methods to represent the effectiveness of safeguards implementation is to evaluate the truth of the proposition: "Any nuclear material in a state is not used for manufacture of nuclear explosive devices." The author proposed a simple evaluation model to calculate it. The model may not be refined but gives a concrete concept for logical fundamentals. From the mathematical viewpoint, fuzzy logic is needed for combining propositions in which truth is less than one. It is possible to define the other combining rules, but the logical framework shown in this paper will be common.

Numerical simulation based on the model shows the effectiveness of integrated safeguards and gives us a hint to make plans for its more efficient implementation.



Note:
1. Calculation result for Integrated Safeguards Implementation is ;
   {Truth value of ~P(NED using HU)}= **Max{0.84+0.1Q, 0.908}**
2. [ ]: Numerical values in the [ ] are in the case of conventional safeguards.
3. *: We assume that inspectorate does not implement indication-detecting activities for this step. Therefore Rj= 0 for the step.
4. Q: Parameter of case studies. Q is defined by Rj when j=O(HU)=O(enrichment).

Figure 4. Numerical Simulation on U-235 Route

An Annotated Taxonomy of Tag and Seal Vulnerabilities

Roger G. Johnston and Anthony R.E. Garcia
Vulnerability Assessment Team
Los Alamos National Laboratory

Abstract

Tags and tamper-indicating seals have important applications for nuclear materials management. Seals are used to detect tampering or unauthorized access, while tags uniquely identify an object or container. Despite the importance of tags and seals, their vulnerabilities have received only limited formal study. Little exists in the way of theoretical guidelines for even discussing, much less characterizing or prioritizing, tag and seal weaknesses. In this paper, we define and discuss 105 different generic attacks on seals and 91 on tags. We comment on these vulnerabilities based on our experience with tags and seals, and with vulnerability assessments. The taxonomy proposed here can be used to clarify vulnerability discussions, to provide a more solid theoretical basis for tag/seal study and development, and to generate a security survey checklist for users of tags and seals.

Introduction

Tags and tamper-indicating seals play an important role in the management of nuclear materials, particularly in the areas of waste management, materials control and accountability, nonproliferation, arms control, treaty verification, international safeguards, records integrity, and counter-terrorism.[1-5] Tags are used to uniquely mark or fingerprint an object or container for purposes of unambiguously identifying it at a later date. Seals are meant to leave unerasable evidence of tampering or unauthorized access. Unlike locks, seals do not necessarily provide resistance to entry. (There are, however, devices called barrier seals that are part lock and part seal.)

Tags and seals are sometimes used interchangeably. This is because a security seal must incorporate some kind of tag-like fingerprint or unique identifier, such as a serial number. Otherwise, the seal can simply be cut off and replaced by a duplicate. Tags, in turn, must either be covert or show evidence if tampered with. Otherwise, they can be removed from one object and placed on another, thus defeating their purpose.

Like all security devices, tags and seals can be defeated—often surprisingly easily.[1, 4-6] In our experience, however, few users of tags and seals are fully aware of their vulnerabilities. Fewer still incorporate vulnerabilities into security planning. Indeed, tag and seal vulnerabilities have received fairly limited attention. There is only a modest theoretical basis for discussing, characterizing, and prioritizing tag or seal vulnerabilities.[1, 4-9]

The purpose of this paper is to propose a taxonomy for tag and seal vulnerabilities. This taxonomy categorizes vulnerabilities in terms of different potential modes of attack. The attacks are identified by a 1-3 character string that appears bold in the text. These character strings form a shorthand notation that is intended to assist in the efficient discussion of vulnerabilities.

The taxonomy presented in this paper may well be incomplete or require future modifications or reorganizations. The hope, however, is that this taxonomy can at least provide a starting point to facilitate more effective discussion of vulnerability issues. It may help to put tamper detection on a more rigorous theoretical footing. This taxonomy may also aid in clarifying issues for users, manufacturers, and developers of tags and seals.

Probably the most practical use for an effective taxonomy is to help generate security survey checklists for security managers. Sample checklists appear in the appendix. Security managers cannot optimize security, nor implement counter-measures, if there are vulnerabilities they do not know about, or have overlooked. The appendix also presents our rankings of what we believe to be the dozen most frequently overlooked critical vulnerabilities associated with the use of tags and seals.

In addition to the taxonomy, we offer comments and general observations throughout this paper about various modes of attack. These comments are based on our previous work with tags and seals for a dozen government agencies and 11 private companies. This work includes testing more than 115 different tags and seals, conducting vulnerability assessments, developing use protocols, assisting with the establishment of seal standards, devising new types of tags and seals, and preparing training materials for tag/seal installers and inspectors.

Risk Concerns

In any public discussion of security vulnerabilities, there is always a concern about helping potential nefarious adversaries ("bad guys") more than security personnel ("good guys"). This should not be a problem here. We present no specific vulnerabilities nor do we discuss specific tags or seals. Indeed, the

generic attack modes discussed here are all (in our view) quite obvious and self-evident to almost anyone with a more than passing familiarity with tamper detection, tags, and seals. Potential adversaries unable to conceive of most of these generic attacks are probably not a substantial security threat to a vigorous tamper detection program.

In general, full knowledge of the wide range of generic tag and seal vulnerabilities is of more help to security managers than adversaries. This is because adversaries usually need to develop only one successful attack strategy for one target. Security managers, on the other hand, must try to simultaneously minimize vulnerabilities for all targets they are responsible for, while being concerned with a wide range of potential adversaries and options. Given this asymmetry between adversaries and security managers, a general awareness of potential vulnerabilities will tend to be more beneficial to the latter than to the former.

Terminology and Notation

In this work, tampering will be defined as gaining unauthorized access for the purposes of stealing, copying, changing, corrupting, supplementing, scrambling, sabotaging, contaminating, spoiling, hacking, damaging, disrupting, or simply conducting an unauthorized examination of the item(s) of interest. The term adversary will be used to mean a would-be nefarious tamperer.

Defeating a seal means gaining entry or access to what the seal is protecting without being detected. Some seal users like to distinguish between defeating a seal and defeating a tamper-detection or security program. The latter may involve, for example, ignoring the seal and attacking the container it is attached to. In this paper, however, we use the term defeating a seal to mean any successful attempt to overcome the purpose of the seal (which is tamper-detection), whether the seal is physically involved or not.

Defeating a tag means overcoming the purpose of the tag without being detected, often by counterfeiting it or removing it from one object and placing it on another.

Attacking a tag or seal means trying to defeat it. A successful attack is also called a defeat.

A passive seal is a seal that does not use electrical power or batteries for continuous operation. Passive seals are often relatively inexpensive and non-reusable. In contrast, active or dynamic seals are more expensive and usually reusable. They involve some form of electronics or electrooptics, often battery-powered. The boundary between a real-time active seal (one that signals tampering immediately) and an intrusion alarm is not always clear.

Some tag or seal attacks require social engineering. By this term, we mean getting insiders to assist the adversary by persuasion, duplicity, converting them to the cause, friendship, romantic/sexual means, intellectual manipulation, emotional or psychological manipulation, bribery, blackmail, extortion, force or threat of force, or posing as a law enforcement or other official to elicit cooperation.

Seal Attacks

Type F (Failure-Mode Attacks)

The first category of seal attacks we identify is designated as type F (Failure-Mode Attacks). These rely on some failure of the tamper detection program. Type F attacks will sometimes be accompanied by a deliberate distraction, or the adversary might wait until one occurs on its own. These attacks require little skill to implement. Either insiders or outsiders may be involved.

Failure-mode attacks can be very effective against security programs that have insufficient planning and training, weak quality control, poorly motivated seal inspectors, or fuzzy thinking. Type F attacks are particularly likely to be executed during inclement weather, organizational upheavals, or when security personnel are shorthanded or the workload is unusually heavy. Security managers sometimes wrongly dismiss type F attacks as 100 percent detectable.

The first type of F attack is particularly easy to execute. For this attack, designated **F1**, the adversary removes the seal and hopes that its absence will be overlooked, simply noted as an inevitable error, or not reported—rather than it being interpreted as a sign of tampering. Indeed, in many security programs, seal inspectors are hesitant to report tampering because of the consternation this causes security managers.[4]

A related attack, designated **F2**, involves the adversary removing the original seal and replacing it with a seal of the same type, but with a different serial number. Again, the adversary hopes this will be overlooked or misinterpreted. Neither should occur in a healthy tamper-detection program.

The type **F3** attack involves the adversary opening a seal, reattaching it to the container, and then severely damaging the seal sufficiently to hide evidence of tampering. The hope is that the seal inspector will conclude the container simply underwent rough handling, instead of tampering. This attack is often accompanied by inflicting substantial collateral damage to the container.

Sometimes (**F4**) an adversary may remove a seal and replace it with an entirely different kind of seal (perhaps with the same serial number) or even a sturdy lock. He hopes that the switch will cause confusion or the presumption of error that prevents the situation from being interpreted as a sign of tampering. The fact that the container in question is still sealed or locked (albeit by the wrong security device) may give the seal inspector a false sense of security.

Attack **F5** involves placing a coating, adhesive, sticker, cover, box, lock, or other hardware over or around the seal. When it is removed at inspection time, it causes enough damage to the seal or seal surface to sufficiently hide evidence of the unauthorized entry that took place. The adversary hopes that the seal inspector is not bothered by the presence of unfamiliar materials on or near the seal.

The **F6** attack involves removing the seal and replacing it with an official-looking document or label signed with a forged signature of some official. It indicates that the container and its contents have already inspected and found to be free from tampering. The adversary hopes this will not be challenged by the seal inspector.

An adversary can also steal the container of interest (**F7**) and hope that its absence will be interpreted as the container simply being misplaced, rather than as evidence of tampering. In certain situations, an adversary may only care about delaying the discovering of tampering, rather than preventing it entirely. The **F7** attack is very effective for such situations.

The final F attack is designated **F8**. For this type of attack, the adversary watches and waits until a mistake is made in the sealing program and exploits it for tampering purposes. An example is to wait until a seal installer is distracted, then tamper with the container before it gets sealed. This type of attack requires patience and flexibility, but it can often be highly effective.

Type P (Pick or Manipulate the Seal Open)

For this attack, the installed seal is picked or manipulated so that it opens without damage and without creating evidence of tampering. Eventually, the seal gets reattached to the container. The designation for this attack is **P**. Based on our experience, this attack is remarkably easy for many types of seals.

Type U (Unseal and then Hide or Repair)

For these kinds of attacks, the installed seal is opened, resulting in damage and/or evidence of entry. After tampering with the items being protected by the seal, the adversary reinstalls the same seal, before or after dealing with the damage or evidence of tampering.

If he fully repairs the damage, the attack is designated **U1**. He may instead undertake a cosmetic cover-up (**U2**) to superficially (but sufficiently) hide the damage so as to avoid detection. Instead of a cosmetic cover-up, he may hide the damage by introducing other damage to the seal that will be misinterpreted as routine wear and tear (**U3**). The damage inflicted for this attack is more subtle than for attack F3.

If opening the seal created evidence of entry (but no damage), the adversary may elect to fully erase the evidence (**U4**). If he instead cosmetically hides the evidence of entry, the attack is designated **U5**. He may also hide the evidence of entry by introducing damage to the seal that will be misinterpreted as routine wear and tear (**U6**).

Attacks U1-U6 can be very effective, especially if the seal inspectors are poorly trained or unmotivated and there is no careful post-mortem examination of the removed seals. Counterfeiting of some seal parts may be useful for these attacks.

Type E (Attacking Electronic Seals)

Type E attacks are relevant only for active seals that use electronics, electro-optics, or wireless communications. These attacks often require surprisingly little sophistication on the part of an adversary, despite the sophistication of the seals.[4]

Direct attacks on the electronic seal components can involve tampering with:

- **E1:** the power source
- **E2:** the optical, electromagnetic, or acoustical signals going into the sensor(s)
- **E3:** the tampering sensor(s)
- **E4:** the signals between the sensor(s) and microprocessor
- **E5:** the microprocessor
- **E6:** the signals between the microprocessor and the annunciator
- **E7:** the annunciator (the portion of the device that reports the alarm or tampering condition)
- **E8:** the signals between the annunciator and the interpretation point
- **E9:** the interpretation station where the alarm condition is received. (In this case, the adversary's goal is to prevent the fact that tampering has been detected from being recognized or acted upon.)

For non-real time electronic seals that store the alarm condition internally, it is possible to erase the stored alarm conditions from memory. This type of attack is designated **E10**.

Type V (Tamper with the Seal Verifier)

The **V** attack is only relevant for (either passive or active) seals that require an electronic or optical reader, i.e., a verifier, to check the seal for tampering. To execute this attack, the adversary tampers with the performance of the reader so that it will fail to report tampering when it has occurred. Tampering with seal data that may be stored inside the reader is covered under category D below.

The V type attack can be easily overlooked by security managers. Seal users must carefully protect readers at all times. It is obviously a blunder to store readers inside rooms or containers sealed with the same type of seal that the reader measures.

Type D (Attack the Seal Data)

Type **D** attacks involve tampering with stored or transmitted information/data about a seal. One method is to tamper with paperwork or computer records about the seal, such as its serial number, color, photograph, or data about the container it has been applied to. This type of attack is designated **D1**. Attacking the seal data stored inside a seal reader is also a valid D1 attack.

Some seal users are careless in how they handle seal serial numbers. They may write seal serial numbers on the outside of containers or railcars instead of keeping careful data records, store paperwork containing the seal serial number inside the container being protected by the seal, improperly safeguard the paperwork, or give the only paperwork containing the seal serial number to the driver of the sealed truck. Such practices make it easy for an adversary (or driver) to replace the seal with the same type of seal having a different serial number, then change the paperwork or the recorded serial number accordingly.

It is also possible (**D2**) to tamper with the communication (or the encryption) of the seal data. When trucks, railcars, or transportainers are sealed, for example, it is common to send information about the seal (such as its serial number) to the final destination via mail, fax, or the Internet. Ideally, such communications should be encrypted or at least well protected.

Adversaries can also tamper with the interpretation, conclu-

sions, and reporting about whether tampering has occurred. This type of attack is designated **D3**. A seal inspector may conclude that tampering has occurred, but this is irrelevant if the information doesn't reach the appropriate supervisory personnel or if they come to the wrong conclusions.

Type S (Sabotage the Sealing Process)

In these attacks, the adversary sabotages the sealing process. These attacks may exploit misdirection, misinformation, distractions, or sleight of hand. They usually require only modest sophistication on the part of an adversary, but have a low probability of success against a competent tamper-detection program.

Attacks S1 through S12 involve insiders. If, during the course of his assigned duties, the insider deliberately fails to close the door on the container being sealed, the attack is designated **S1**. He may also deliberately fail to seal all doors (**S2**), seal the wrong container (**S3**), use the wrong seal (**S4**), knowingly report incorrect seal data (**S5**), or fail to properly install the seal (**S6**). For attacks S1 and S2, the correct doors may eventually get closed and properly sealed by the adversary's accomplices. In the case of attacks S4 and S6, the correct seal might eventually get placed on the container correctly at a later time to avoid detection.

An (insider) adversary may pretend to accidentally damage the seal in order to hide evidence of tampering (**S7**). Running into the seal and container with a forklift would be a common strategy. The insider could also pretend to accidentally remove the seal prematurely, before it can be fully inspected. This attack is designated **S8**.

Insiders can tamper with cargo by putting the wrong objects inside a container, truck, or railcar during loading, prior to sealing. This type of attack is designated **S9**. If the wrong number of objects are placed inside the container, truck, or railcar during loading, the attack is designated **S10**.

Similarly, insiders can remove the wrong objects after the container has been officially unsealed (**S11**), or remove the wrong number of objects (**S12**).

Attacks S13-S16 can involve either insiders or outsiders. For **S13**, the adversary tampers with the training program for seal installers and inspectors, and/or with the seal user's understanding of the proper seal protocols and security procedures. If the adversary creates propaganda to damage the seal's reputation in the mind of the seal user, he may create apathy and carelessness. This is attack **S14**. Also, generating agitation and malcontent among security personnel may compromise their performance (**S15**).

Another type of attack (**S16**) along these lines is to create repeated false alarms by damaging or opening seals and containers not of interest to the adversary, by tampering with seal data, or mixing up unused seals, thus undermining the seal user's confidence in the seals and the overall tamper-detection program. The S16 mode of attack is the equivalent of a common trick of burglars: setting off the burglar alarm for three or four nights in a row. Eventually, the police or security personnel respond less quickly, or even quit responding entirely, making the real burglary attempt easier a few nights later.

Type B (Backdoor or Prior-to-Use Attacks)

The next general category of attack, which we designate as type B, involves putting a backdoor or defect into a seal. This means that an adversary modifies the seal prior to use. The goal is to permit easier, undetected access at a later time. Vulnerabilities associated with these attacks can be mitigated if seals are carefully protected at all times prior to use, and thoroughly inspected immediately before being installed. Most seal users do the former, but few do the latter.

There are a number of different times that a backdoor attack can be implemented:

B1: Adversaries can put in a backdoor during the seal design process. In this case, a defect is deliberately designed into the seal, which can be exploited at a later date.

The adversary may instead introduce exploitable defects into seals after the design is finalized and:

B2: prior to when the seal is manufactured, such as by tampering with seal parts or raw materials
B3: during the manufacturing process
B4: while the finished seals are in storage at the production plant
B5: in transit between the manufacturer and the seal vendor or distributor
B6: while at the vendor
B7: in transit between the vendor and the seal user's receiving department or loading dock
B8: at the seal user's receiving department or loading dock
B9: in transit between the receiving department (or loading dock) and the parts department
B10: at the seal user's parts department
B11: in transit from the parts department to the seal user's secure storage area
B12: at the seal user's secure storage area
B13: in transit from the storage area to the seals checkout point (where seal installers obtain the seals prior to sealing containers)
B14: at the seal user's checkout point, prior to the seals being checked out by seal installers
B15: just prior to when the seal is installed on a truck, railcar, or container.

Note that a given security program may not include all of the above steps. For example, many seal users order directly from the seal manufacturer, so there is no vendor or distributor. Also, the storage area and the seal checkout point are the same location for many seal users.

There are two other kinds of type B attacks (B16 and B17) that are less physical. An insider working at the seal vendor can place seal orders with the manufacturer that are designed to compromise seal security (**B16**). For example, the insider might deliberately order seals with duplicate serial numbers. (A responsible seal manufacturer should not permit this.) In a related attack, the insider works for the seal user, rather than the seal vendor (**B17**). He orders seals from the seal vendor or man-

ufacturer in a matter that compromises security.

We believe that, in general, potential attacks B3-B10, and B15-B17 probably deserve more attention than they traditionally receive from security managers. In particular, the commercial market for tamper-indicating seals is a very competitive, low profit-margin business, especially for passive seals. This is exacerbated by the fact that many seal customers appear to choose seals primarily on the basis of unit cost, rather than performance. As a result, it is not clear that seal manufacturers and vendors implement effective security at their facilities, or can afford to do so. On the other hand, most seal manufacturers employ a relatively small number of people. This may make it difficult for an adversary to blend in with authorized factory personnel.

Type R (Replicate the Seal)

Another major category of seal attack, which we designate with the letter R, involves replicating the seal. The original seal is removed from the container by the adversary and replaced with a duplicate seal.

Seals can be replicated a number of different ways. An adversary can order duplicate seals (e.g., with the same serial numbers) from an original manufacturer by:

R1: posing as a legitimate vendor
R2: posing as the original seal user.

Attacks R1 and R2 differ from attacks B16 and B17 discussed above in that B16 and B17 require the assistance of insiders. R1 and R2, in contrast, involve the adversary (as an outsider) posing as authorized personnel.

An adversary might also use the seal manufacturing facility in person to replicate seals surreptitiously:

R3a: during regular business hours
R3b: after hours, by breaking into the factory.

Again, it is not clear that manufacturers of commercial seals routinely employ sufficient security to prevent these kinds of occurrences.

Yet another approach is for an adversary to use non-surreptitious means to get the factory to produce duplicate seals (without posing as the original seal user). This attack is designated **R4**. This could be accomplished by getting the seal manufacturer (or personnel within the factory) to replicate seals voluntarily, or by using social engineering.

Another approach (**R5**) that is at least theoretically possible is for the adversary to steal the manufacturing equipment from the factory and replicate seals at his own location.

In general, type R replicating attacks can be effective, inexpensive, and relatively easy to implement. They probably do not generally received sufficient attention, particularly given that the security at many seal manufacturers and vendors may be suspect.

Type C (Counterfeit the Seal)

Type C attacks involve counterfeiting the seal. Counterfeiting differs from the replicating (R) attacks discussed above in that the R attacks create the duplicate seals using only the original manufacturer's production facilities and equipment. Type C attacks require additional or different equipment and techniques.

Seal vendors and manufacturers often stress the difficulty of counterfeiting their seals. This is often overstated. Counterfeiting—while not the automatic choice of most adversaries—is frequently easier than many imagine. Some counterfeiting attacks involve replacing the fingerprint (unique identifier) on an unused seal, such as the seal serial number, with a counterfeit fingerprint, or with one lifted from the original seal. In some situations, it may not be necessary for the adversary to counterfeit the seal fingerprint at all. He may only need a seal that looks similar, or that has a similar, though not identical, fingerprint. This is particularly the case with type D attacks discussed above.

If the adversary makes the seal from scratch (without modifying an existing seal or using the resources of commercial seal manufacturers), the attack is designated **C0**.

An adversary may, however, make a counterfeit seal by modifying existing seals, even using seals made by a different manufacturer. This is often practical because many passive seals use similar or identical materials, parts, and designs, despite being made by different companies. An adversary may obtain unused seals from a variety of sources for the purposes of modifying them to make counterfeits. These sources include the original manufacturer, the vendor, a competing manufacturer, the seal user he intends to attack, or a different seal user.

Seals obtained from the original manufacturer can be obtained in a variety of ways:

C1a: for free (Manufacturers are usually eager to provide free seal samples to potential customers. Sometimes these free samples are marked as such, or differ in some way from the purchased product. Often, however, the free samples are either identical to the purchased product, or so close that they are useful for counterfeiting purposes.)

C1b: by openly purchasing the seals. (In our experience, seal manufacturers are not always as careful to protect seal logos and serial numbers as they should be, claim to be, or promise. It is often possible to obtain seals with almost any logo and/or range of serial numbers.)

C1c: via social engineering
C1d: by theft.

Similarly, seals for counterfeiting purposes can be obtained from a seal vendor in different ways:

C2a: for free
C2b: by openly purchasing the seals

C2c: via social engineering
C2d: by theft.

The seals can instead be obtained from a (different) competing manufacturer in various ways:

C3a: for free
C3b: by openly purchasing the seals
C3c: via social engineering
C3d: by theft.

The adversary can surreptitiously make seals himself at a competing manufacturer's factory:

C4a: during regular business hours
C4b: by breaking into the factory after hours.

If he instead steals the competing manufacturer's production equipment for use elsewhere, the attack is designated **C5**. (Presumably there is no need to allow for C attacks involving the original manufacturer's factory. These are covered under R attacks above. If an adversary has access to the original factory or production equipment—as in attacks R3a, R3b, and R5—he can replicate the seals exactly, rather than making a similar seal and modifying it later.)

Unused seals for counterfeiting purposes may be obtained from the seal user a number of ways:

C6a: for free (Some seal users will happily provide free, unused samples of their seals if asked properly, or if the requester assumes a false identity.)
C6b: by purchasing the seals
C6c: via social engineering
C6d: by theft.

Unused seals for counterfeiting purposes may be obtained from an alternative seal user in these ways:

C7a: for free
C7b: by purchasing the seals
C7c: via social engineering
C7d: by theft.

The above C attacks involve the use of unused seals. Adversaries can also make counterfeit seals from used seals or seal parts. These can be obtained from the seal user:

C8a: by the seal user willingly providing them
C8b: (openly or covertly) because the seal user improperly discarded used seals. (While most seal users are careful about protecting unused seals prior to use, many are careless in how they dispose of used seals. It is common in various applications to find seals that have been cut off from trucks or railcars lying around loading docks, or disposed of in the trash. Used seals must be thoroughly destroyed or archived; slicing them up or punching a hole in a used seal is not sufficient to destroy their value to an adversary.[4])
C8c: via social engineering
C8d: by theft.

If the used seals or seal parts are obtained from a different seal user (one other than the intended attack victim), the attacks are designated as follows:

C9a: if the seal user willingly provides the used seals or seal parts
C9b: if the seal user improperly discarded the used seals
C9c: if social engineering is used to obtain the used seals or seal parts
C9d: if theft is used to obtain the used seals or seal parts.

Type A (Alternative Attacks—Bypassing the Seal)

The alternative attacks category involves bypassing the seal, seal control program, or seal data. If an adversary elects to use A-type attacks, the seal has won, that is, it has fulfilled its function. These are, nevertheless, viable attacks that seal users may overlook.

An adversary may elect to attack the top, sides, or bottom of a container, gaining access to what the seal is protecting without ever touching the seal. Such container attacks are designated **A1**. If the adversary attacks the container door or hinges instead, the attack is **A2**. Attacking the locking mechanism or hasp on the door is designated **A3**.

Attack **A4** is a stay-behind attack for large containers or rooms. The adversary gets himself placed surreptitiously inside the container or cargo, and tampers with its contents after the container is sealed. He then hides in or among the container contents, hoping to escape unnoticed or unchallenged when the container is eventually opened. Midgets, small women, children, or contortionists may be employed.

Attack **A5** is a stay-behind attack that involves a machine. The adversary surreptitiously places a machine inside the container or inside some of the cargo. This machine is used to tamper with the container contents after the container is sealed. The machine may be a robot that operates on its own, or it may be controlled from outside the container under wireless communication from the adversary. After completing tampering, the machine hides in or among the container contents, or disassembles itself. The adversary hopes it will go unnoticed or unchallenged when the container is eventually opened. For some applications, the adversary in attacks A4 and A5 may not care that the tampering is eventually discovered if it can go undetected for a time.

Personnel Who Execute Attacks

Some attacks can be further sub-categorized by the type of personnel who (primarily) execute the attack and, in the case of insiders, their motivation. The motivation for insiders should be of concern to security managers because they may be able to influence it. Security managers, however, usually have no con-

trol over the motivations of outsiders, so we do not consider outsider motivation here.

When it is useful to characterize attack personnel, we propose the following categories. The symbols in bold are the shorthand notation for each type of attacker. Categories 0-4 involve outsiders; categories 5 and 6 are for insiders.

If an outsider works surreptitiously from the outside, the personnel designation is **0**. If instead the outsider gets a job as an insider, and attacks during the course of assigned duties, the designation is **1**. If the outsider gets a job as an insider and attacks outside of his assigned duties or work area, the category is **2**.

An outsider posing as an insider is denoted with a **3**. An outsider posing as an authority figure (law enforcement officer, fire fighter, company executive, etc.) is designated **4**.

Category 5 attacks involve an insider who attacks or assists the adversary during the course of his regular assigned duties. The primary reason he assists may be because of:

- **5a:** the fact that he already is a member of the adversary's team
- **5b:** bribery
- **5c:** blackmail
- **5d:** duplicity, i.e., being unaware of the implications of assisting the adversary
- **5e:** extortion
- **5f:** force or threat of force
- **5k:** being converted to the cause
- **5m:** mental manipulation
- **5p:** persuasion
- **5q:** friendship
- **5r:** romantic or sexual motivation.

Category 6 attacks involve an insider who attacks or assists the adversary outside of his regular assigned duties or normal work area. The primary reason he assists may be because of:

- **6a:** the fact that he already is a member of the adversary's team
- **6b:** bribery
- **6c:** blackmail
- **6d:** duplicity, i.e., being unaware of the implications of assisting the adversary
- **6e:** extortion
- **6f:** force or threat of force
- **6k:** being converted to the cause
- **6m:** mental manipulation
- **6p:** persuasion
- **6q:** friendship
- **6r:** romantic or sexual motivation.

Tag Attacks

For tags, the taxonomy includes the same F, E, V, D, B, R, and C attack categories defined above for seals. Seal attack categories U and A, however, are not relevant for tags. Seal attack categories P and S have to be modified for tags as follows:

Type P (Remove and Place the Tag on a Different Object)

Attacks P1-P4 are probably the most likely type of tag attacks. For these attacks, the tag is removed from the object it is attached to and placed on a different object (or container). This may or may not result in damage or evidence of tampering. If it does not, the attack is designated as **P1**. The adversary hopes in a P1 attack that the damage or evidence of tampering will be overlooked or slight enough to avoid detection.

If damage or evidence of tampering occurs, this can be dealt with by fully repairing the damage or evidence of tampering (**P2**). If instead the damage or evidence of tampering is cosmetically hidden to avoid detection, the attack is designated **P3**. The **P4** mode of attack involves hiding the damage or evidence of tampering by introducing deliberate damage to the tag that will be misinterpreted as routine rough handling.

Type S (Sabotage the Tagging Process)

In these attacks, the adversary sabotages the tagging process. These attacks may exploit misdirection, misinformation, distractions, or sleight of hand. They usually require little sophistication on the part of an adversary, but have a low probability of success against a competent security program.

Attacks S1 through S6 involve insiders. If the insider puts the tag on the wrong object or container, the attack is designated **S1**. Deliberately using the wrong tag is **S2**. Knowingly reporting incorrect tag data is **S3**, while failing to properly install the tag is **S4**.

The insider adversary may pretend to accidentally or inadvertently damage the tag in order to hide evidence of tampering (**S5**). The insider could pretend to accidentally remove the tag prematurely, before it can be fully inspected. This attack is designated **S6**.

Attacks S7 through S10 can involve insiders or outsiders. Tampering with the training program for tag installers and inspectors, and/or with the tag user's understanding of the proper protocols is attack **S7**. Creating propaganda to damage the tag's reputation in the mind of the user, thus creating apathy and carelessness is attack **S8**. Attack **S9** involves creating agitation and malcontent among the tag user's security personnel so their performance is compromised. Attack **S10** is about generating repeated false alarms by damaging or removing tags, tampering with tag data, or mixing up unused tags, thus undermining the user's confidence in the tags and the overall tagging program.

Examples of Shorthand Notation

In using our shorthand notation for seal or tag attacks, it is necessary to specify whether the attack is on a tag or a seal (unless the context is clear). This is because a given tag attack may have the same letter designation as a seal attack, yet involve a very different strategy.

Here are some examples of the notation for seal attacks:

F2: The adversary removes the seal from its container and replaces it with the same type of seal having a different serial number. The personnel performing this attack are not specified.

F2-3: This is the same F2 attack, except that we now specify that the attack is carried out by an outsider who gains access to the seal by posing as an insider (personnel category 3). The dash

is used to separate the attack designator (F2) from the personnel designator (3).

F2-5f: This time the F2 attack is executed by an insider—working within his assigned work area and range of duties—who has been compromised by force or threat of force (5f).

C1d/D1: This attack involves two different vulnerabilities. Attacks that combine two (or more) of the attack categories are denoted with a slash between the designation strings. For this attack, the adversary steals a seal from the manufacturer to make a counterfeit (attack C1d), then tampers with the seal user's paperwork so it reports the serial number of the counterfeited seal (D1). We do not specify the personnel involved.

C1d-4/D1-5k: Here, we want to be more specific about who performs the attack. In this case, the seal was stolen by an outsider who gained access to the factory by posing as an authority figure (-4), yet the tampering with the seal data was done at the seal user's location by an insider during the course of his regular assigned duties, having been converted to the adversary's cause (-5k).

Concluding Remarks

This paper has described and discussed 105 different generic attacks on seals and 91 on tags. If combination attacks, plus the different possible personnel and their motivations are included, the number of possible generic attacks is in the thousands.

The probabilities of the generic attacks discussed in this paper vary widely. Attack likelihoods depend critically on details of the application, the tags or seals employed, economics, personnel, and the overall security program. We nevertheless attempt in the checklists to identify what we believe to be the dozen most critically overlooked potential attacks on tags and for seals used for nuclear applications. (A rank of '1' means the attack is the most critically overlooked.) These choices are based on our experience with tags and seals and with tamper-detection programs. We make no attempt to justify our choices here; they are clearly open for debate and will differ significantly from one security program to another. Our intent is merely to emphasize those potential vulnerabilities that are likely to be worth extra attention.

In our experience, most of the vulnerabilities covered in this taxonomy can be dramatically reduced or eliminated by employing the proper counter-measures, including an awareness that the vulnerabilities exist. Counter-measures are often surprisingly inexpensive and simple to implement. Legitimate tag and seal users are welcome to contact the authors to discuss these and other tamper-detection issues.

Roger G. Johnston is team leader for the advanced chemical diagnostics and instrumentation group at Los Alamos National Laboratory. He also heads the LANL vulnerability assessment team. His research interests include specialty tools and instrumentation, laser interferometry, and tamper detection. Johnston earned a B.A. from Carleton College in 1977, and M.S. and Ph.D. degrees in physics from the University of Colorado in 1983. Prior to joining LANL, Johnston conducted research at Argonne National Laboratory, NASA, and N.V. Philips in the Netherlands.

Anthony R.E. Garcia is a senior technician in the advanced chemical diagnostics and instrumentation group at Los Alamos National Laboratory, and a member of the vulnerability assessment team. He has contributed to research and development at LANL in the areas of superconductivity, electron microscopy, vacuum technology, electrooptics, laser interferometry, chemical sampling, tool design, tamper detection, and security.

Acknowledgements

This work was performed under the auspices of the U.S. Department of Energy. Janie Enter and Anna Nogar provided input for this paper.

References

1. C.A. Sastre, "The Use of Seals as a Safeguards Tool," Report BNL 13480, Brookhaven National Laboratory (1969).
2. NFESC, "DoD Antipilferage Seal User's Guide," Naval Facilities Engineering Service Center, Port Hueneme, California USA, (1997).
3. IAEA, "The IAEA's Safeguards System: Ready for the 21st Century," Report 97-03433, International Atomic Energy Agency, Vienna, Austria (1997).
4. R.G. Johnston, "The Real Deal on Seals," *Security Management* 41 (No. 9): 93-100 (1997).
5. R.G. Johnston, A.R.E. Garcia, and W.K. Grace, "Vulnerability Assessment of Passive Tamper-Indicating Seals," *Journal of Nuclear Materials Management* 224: 24-29 (1995).
6. R.G. Johnston and A.R.E. Garcia, "Vulnerability Assessment of Security Seals," *Journal of Security Administration* 20 (No. 1): 15-27 (1997).
7. J.L. Rosette, "Development of an Index for Rating the Effectiveness of Tamper-Evident Packaging Features," Masters Thesis, California Coast University, Santa Ana, CA (1985).
8. J.L. Jones, "Improving Tag/Seal Technologies: the Vulnerability Assessment Component," Report 95/00599, Idaho National Engineering Laboratory (1996).
9. R.G. Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals," *Journal of Testing and Evaluation* 25, 451-455 (1997).

Activity-Based Costing and Relevant Cost Analysis: An Example of Protective Force Services and Security Upgrades

Dennis F. Togo, Ph.D.
University of New Mexico

Claude S. Potter, MBA
Sandia National Laboratories

Abstract

National laboratories are being encouraged to become more cost effective but their accounting data often impedes identifying the cost of current operational activities. The practice of activity-based costing was developed in the private sector in response to managers' needs for more accurate product and service costs. While ABC is not likely to replace one's cost accounting system, it has proven to be useful in strategic decision-making. This paper provides an overview of ABC, the steps to implement its use and an example within security operations.

ABC estimates for protective-force activities were used to illustrate a strategic decision for security upgrades in meeting higher protection standards at a typical nuclear materials research site. Relevant cost analysis was performed with spreadsheet models for three alternative physical protection upgrades: technology, facility modifications, and underground facility. The results of the analysis provided the basis for selecting a cost-effective approach to meet increasing protection standards.

Introduction

The U.S. Congress has targeted national laboratories in an attempt to control and reduce government spending and encouraged them to adopt cost-cutting practices of profit-oriented entities. Laboratories have generally responded by focusing on support activities before reducing critical research activities in trying to reduce costs. At the same time, government requirements placed on research performed at the laboratories have been increasing. In particular, nuclear materials research has seen a heightening of safety standards in this period of sought after cost reduction.

Laboratories that conduct nuclear materials research incur significant indirect costs in their safeguards and security divisions. Some nuclear materials research sites have closed because of the high and increasing costs of S&S costs. The cost increases are attributed to ever-increasing protection standards and an aging nuclear research facility. Hence, national laboratories are faced with a two-fold problem: the immediate problem of minimizing and controlling security costs for nuclear research, and at the same time maintaining a nuclear research capability into the future.

The largest cost for S&S in securing an area containing nuclear materials is for the protective force. The ProForce consists of highly trained security officers who control entry into and exit from secured areas, monitor communications for the area, and provide emergency response when necessary. In reviewing the ProForce for possible cost reductions, S&S managers are hampered because costs are aggregated within traditional accounting-reporting functions that provide very little information on the cost of specific security activities.

In the next sections, activity-based costing is described with steps to derive estimates for activities. An example for ABC use and relevant cost analysis is presented for ProForce activities involving a strategic decision for alternative security upgrades. Relevant cost analysis using ABC data is performed with spreadsheet models for three alternative physical protection upgrades. The relevant cost analysis provides a methodology for selecting a cost-effective approach to meet increasing protection standards.

The three operational S&S groups usually found at a nuclear materials research complex are classified as ProForce, material control and accountability, and electronic security systems. ProForce operations are the focus of this illustration because it usually represents nearly four times the cost of the other two functions, and its highly variable cost structure presents the more obvious opportunities for reducing costs. Furthermore, this study focused only on an area (Area X) within a facility having a concentration of special nuclear materials.

Activity-Based Costing Overview

The objective of ABC is to determine a truer cost of manufacturing a product or providing a service. Hence, ABC focuses on the activities in supplying a product or service, and employs the activities' drivers in assigning cost. Consequently, managers provided ABC information are more knowledgeable about

incurring costs in comparison to traditional costing systems that report cost by production or selling functions rather than by activities. Managers provided ABC information focus on reducing operational costs by reducing the consumption of cost drivers, eliminating nonvalue-added activities, or strategically combining value-added activities.

An ABC system (Figure 1) is based on an understanding of the cause-and-effect relationship between the resources consumed in the performance of business activities, and the products and services that are the output of these activities. ABC initially traces direct costs wherever possible to the output products or services. Then, ABC employs a two-stage procedure in assigning indirect allocable costs to products or services. First, a process mapping of resources consumed in the performance of identified activities becomes the basis for allocating resources to activity cost pools. Second, ABC allocates the cost pool using a predetermined activity rate whenever products or services consume activities. Thus, under the ABC system, direct costs are traced to the product or service, and indirect costs are allocated by the activities required to produce them.

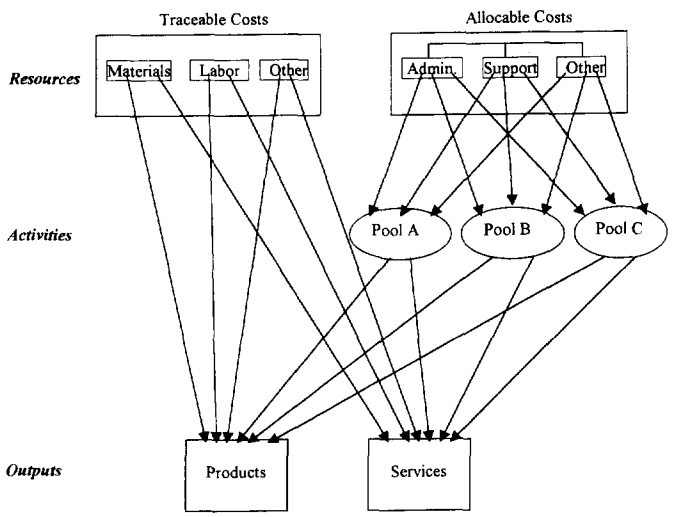


Figure 1: Activity-Based Costing

For each activity cost pool, cost drivers allocate costs to the product or service. A cost driver is any factor that causes a significant change in the cost of performing an activity. An activity connotes people or machines doing work. The term "driver" refers to the work being done (e.g., number of purchase orders completed, welds made, or customer telephone calls answered). An activity may have multiple cost drivers. For example, costs incurred for specific guard patrols are likely to be driven by the frequency and the route of the patrol.

In contrast to traceable direct costs (e.g., direct materials, direct labor, and depreciation of dedicated equipment), the causal link between allocable indirect/overhead costs and the activities performed are seldom clearly established. Traditional costing methods frequently use volume-related measures (e.g., square footage, number of employees, and sales volume) to allocate indirect costs across all products or services provided. This spreading of indirect costs has lead to inaccurate cost data where multiple products or services use overhead costs differently. An important benefit of ABC is that it provides a mechanism by which indirect/overhead costs can be attributed to specific activities and then allocated based on the consumption of these activities. ABC provides a clearer understanding of where overhead resources are being used.

The use of ABC, whether as a costing system or a management tool, has resulted in several improvements in accounting. First, more direct costs are identified and now traced to the outputs of the organization. Second, cost pools have increased in number and there is greater homogeneity within each cost pool associated with an activity. A homogeneous cost pool suggests that a common cost driver drives the contained costs. Third, the cost drivers of the activity pools are more in sync with operations in comparison to the traditional volume-related bases. These improvements in accounting when ABC is adopted provide managers with what the operations people already knew — that different products and services consume different amounts and types of resources. A common finding among companies adopting ABC is the undercosting of low volume product or services. Consequently, high-volume product or services are often found to be overcosted.

The managerial benefits of adopting ABC include more accurate cost information for pricing, more accurate profit analysis by product, customer, or department, targeted cost reduction opportunities, more cost control, better planning, improved organizational cost structure, and better product-mix decisions. Perhaps the greatest benefit to a company adopting the concepts of ABC has been the acquisition of a new managerial perspective to operations of the organization. By focusing on activities as the drivers of cost, managers can reduce and control costs by identifying the cost drivers of key activities and finding ways to reduce their consumption. In addition, ABC helps managers to reduce costs assigned to the activities by reexamining the activity and eliminating nonvalue-added activities. Consequently, ABC enables managers to make better decisions because they better understand what drives the different costs for different products and services.

Steps in Applying ABC

An activity driven approach to management can be easily adopted. Implementing ABC involves the following steps, summarized in Figure 1.

1. Identify the products or services (outputs) of the company.
2. Identify the resources consumed to complete the products or services.
3. Determine traceable direct costs (e.g., labor and materials) and assign to the products or services.
4. Identify activities required to complete the products or services, and a cost driver for each activity.
5. Link remaining resources to outputs by first mapping resources to activity cost pools, and then allocating the cost pools to the products or services using cost drivers.

Table 1: Option 0 - Baseline
Fiscal Year 200X Security Estimate of Baseline Protection Costs in 1,000s (K)

Organization	FTE Req.	FTE Rate	Labor Cost	DS/DC[1]	Total
Protective Force					
Security Response Team (SRT):[2]				*$478*	$478
Captain	*1*	*$85*	$85		$85
Lieutenant	***11***	*$80*	$880		$880
SPO III	*77*	*$62*	$4,774		$4,774
Staffing Shortage Overtime Premium[3]			***$917***		$917
Communicator	*12*	*$55*	$660		$660
Supply	*1*	*$55*	$55		$55
Administration	*3*	*$64*	$192		$192
Training	*4*	*$83*	$332		$332
Equipment & Space				*$367*	$367
Subtotal	**109**		**$7,895**	**$845**	**$8,740**
Electronic Security Systems					
Technical	*3*	*$74*	$222	*$70*	$292
Administration	*1*	*$128*	$128		$128
Contractors				*$17*	$17
Training				*$20*	$20
General & Administration & Space				*$65*	$65
Subtotal	**4**		**$350**	**$172**	**$522**
Material Control & Accountability					
Technical	*2.3*	*$87*	$200		$200
Support	*2.2*	*$86*	$189		$189
Equipment & Space				*$62*	$62
Subtotal	**4.5**		**$389**	**$62**	**$451**
Security Requirements & Planning					
Support	*1.4*	*$82*	$115		$115
SSSP	*0.2*	*$90*	$18		$18
Space			*$4*		$4
Subtotal	**1.6**		**$137**	**$0**	**$137**
PSAP Program Costs					
Personnel Security	*1.3*	*$64*	$83		$83
Line Costs	*0.5*	*$68*	$34		$34
Medical	*0.8*	*$78*	$62		$62
Subtotal	**2.6**		**$180**	**$0**	**$180**
Total	**122**		**$8,951**	**$1,079**	**$10,030**

Notes
1. Direct Services and Direct Costs
2. 24 hour-a-day, 7 day-a-week positions assume a 5.5 FTE.
3. While 109 FTEs are required to fill needs, only 80 positions are currently filled. The SRT overtime premium reflects the shortage of 2 Lieutenants and 27 SPO IIIs filled at 1.5 of regular rates.

	FTE Req.	Assigned	Shortage	1/2 FTE	O/T Prem.
Lieutenant	*11*	9	2	$40	$80
SPO III	*77*	50	27	$31	$837
Other SRT Personnel	21	21	0		$0
Total	**109**	**80**	**29**		**$917**

6. Manage the business process activities required to produce the products and services.

In the following section, an example of how ABC data could be used for a key managerial decision is presented.

Example of ABC Usage and Cost Analysis: Security Upgrades

Problem Description

National laboratories of the U.S. Department of Energy are finding it economically difficult to comply with ever-increasing protection standards for nuclear research. Laboratories have met the higher standards usually by adding more ProForce personnel. However, this response has often been troublesome, as some laboratories have closed their nuclear research efforts because of the high and increasing security costs. Why do the laboratories respond with expensive ProForce personnel and how do they effectively counter the trend of responding with more ProForce personnel?

The decision by security managers to add more ProForce in response to heightened standards is driven primarily by the antiquated facility housing the nuclear-research capability. An analogy of this problem is that of requiring air bags, antilock brakes and fuel injection in a 30-year-old car. These safety and performance innovations were never projected for the car built 30 years ago. Furthermore, even though these innovations can be added to the car, the effectiveness of the new technology is hindered and the car's operating costs are adversely impacted by this mismatch of technology. Hence, the laboratories are faced with the immediate problems of minimizing and controlling operating costs for its nuclear-research capability, and also the problem of maintaining this capability into the future.

On the other hand, there is a bright side for opportunistic laboratories made available by the demise of other nuclear research sites. Research conducted elsewhere is likely to be transferred to cost-efficient sites. Future nuclear research in the DOE would probably be conducted at only cost efficient sites, as the cost of starting up a previously closed site is likely to be prohibitive. Laboratories should feel an urgency to seek out cost-effective ways to meet increasing protection standards if for no other reason than to retain a nuclear-research capability within the DOE.

Scope

This study will examine significant proposed changes to the protective service operations at the nuclear materials research facility. As expected, the three options presented by security's management focus on major protection system changes to the facility housing the nuclear-materials research capability. Each option represents a different approach to the cost structure of protective operations and to potential cost savings. In particular, the level of ProForce staffing will be significantly impacted by the three options. The purpose of this example is to perform a cost/savings analysis of the three options in Area X of a nuclear-materials research facility.

The three options will be compared to estimates for baseline security costs for fiscal year 200X in ranking the cost effectiveness of each option. The analysis uses available cost estimates that were prepared using ABC, especially the cost of ProForce activities in Area X. As a deliverable to security management and an integral part of this study, a spreadsheet was prepared that models the quantitative cost/savings analyses. The spreadsheet found in a following section allows managers to make changes to key input estimates when performing scenario analysis.

Defining the Options

Option 0 — Baseline identifies 200X cost estimates for ProForce, electronic security systems, material control and accountability, security requirements and planning, and the personnel security assurance program. The annual costs would be ongoing over the remaining 10-year life of the current facility.

Option 1 — Technology upgrades emphasizes evaluating, designing, and implementing technologies currently available for delay, detection, and response protection systems. These systems would be installed at the existing facility with minimal construction changes to the facility.

Option 2 — Facility modifications proposes to construct major additions to the existing facility, including the technology upgrades of Option 1, to enhance delay, detection, and response protection systems.

Option 3 — Underground facility proposes building a new, state-of-the-art underground facility and moving operations to this new facility. In contrast to the estimated 10 years remaining life of the current facility, the UGF would have a projected life of 30 years.

Key Assumptions for Options

Key assumptions for each option are presented below. These key assumptions are highlighted in the following spreadsheets as bold and italicized. A common assumption to Options 0, 1, and 2 is that the remaining life of the current facility is 10 years. An assumption common to Options 1, 2, and 3 is that a 2-year period is needed to complete the system upgrade.

Another important assumption is the ABC cost of ProForce activities in Area X. Without disclosing the specific activities for guard patrols, communication posts, and supervision and training, Table 1 lists the overall staffing levels of the ProForce and estimated yearly ABC FTE rates used in the cost analysis. Table 1 also lists any other expected costs to be incurred for the ProForce. Traceable costs, for instance wages and labor-driven overhead costs, were assigned to outputs such as guard patrols and communication posts. Other indirect costs were allocated to outputs on the basis of FTE consumed.

Option 0 - Baseline

1. The FTE Required estimates 11 lieutenants and 77 SPO IIIs to meet current protection standards. The FTE required is based on 2 Lieutenant and 14 SPO III patrols that are 24-hours and seven days a week, with each patrol having a 5.5 FTE equivalent.
2. The current staffing of SPO IIIs and lieutenants are

Table 2: Option 1 - Technology Upgrades (K)

Activity	FTE Req. (Months)	FTE Rate	Labor Cost	DS/DC	Total
Consulting and Department Support:					
Protection Upgrade Delay Consulting	*3*	*$225*	$56		$56
Recapture/Recovery Evaluation	*2*	*$225*	$38		$38
Joint Tactical Simulation (JTS) Support	*3*	*$225*	$56		$56
Security Requirements & Planning Support	*3*	*$90*	$23		$23
Protective Force Support	*3*	*$83*	$21		$21
Reactor Operations Support	*3*	*$280*	$70		$70
Vault 1 Upgrade:					
Conceptual Design	*2*	*$225*	$38		$38
Command and Control Scoping[1]					$0
Design and Installation[2]				*$125*	$125
Reactor and Plate Tie downs	*3*	*$225*	$56	*$35*	$91
Vault 2 Upgrade:					$0
Conceptual Design	*2*	*$225*	$38		$38
Command and Control Scoping	*4*	*$225*	$75		$75
Design and Installation[3]				***$800***	$800
Response Force Technologies:					
Facility Modifications Design	*2*	*$225*	$38	*$20*	$58
Installation of Facility Mods					
Breaching Techniques	*2*	*$225*	$38	*$20*	$58
Automated Response Systems[4]	*4*	*$225*	$75	*$100*	$175
Design				*$20*	$20
PIDAS 1 Upgrade and Reconfiguration				***$750***	$750
Total			**$620**	**$1,870**	**$2,490**

Notes:

1. Command & Control (C^2) Scoping cost for Vault 1 Upgrade uses the same system developed for Vault 2.
2. C^2 system costs assume leveraging from a system implemented at another site.
3. Design and Installation estimate combines internal and external contractor costs.
4. Auto response system costs assume purchasing equipment from vendor instead of borrowing.

Added Annual Costs:	
Technical maintenance and quality testing	*$40*
Trouble shooting	*$10*
Pro Force training and performance testing	*$20*
Total Added Annual Costs	**$70**

Net Annual Savings:		
SPO III FTE[a]	*2.5*	*$155*
Portion of staffing shortage		$78
PSAP savings		$0
Total Annual Savings		**$233**
Less Added Annual Costs		**$70**
Net Annual Savings		**$163**

Cost Analysis Over 10-yr Life of Upgraded Facility:	
Net Annual Savings	$163
Estimated Life of Upgraded Facility	10
Savings over Life of Upgraded Facility	$1,630
Less One-Time Costs	$2,490
Net Cost Over 10-yr Life	**-$860**

Payback Period	
One-Time Costs	$2,490
Net Annual Savings	$163
Payback Period (years)	**15.3**

Note a - Similar technology upgrades have led to 2.5 FTE reductions in SPO III.

below the FTEs required for the patrols currently in place. Actual ProForce levels present a staffing shortage of 2 lieutenants and 27 SPO IIIs. This staffing shortage incurs an overtime-premium cost of $917,000, calculated as Lieutenant: 2 X .5 X $80,000 = $80,000, and SPO III: 27 X .5 X $62 = $837,000

Option 1 - Technology Upgrades

1. The design and installation cost of vault 2 upgrades is $800,000.
2. The PIDAS 1 upgrade and reconfiguration is estimated at $750,000.
3. Command and control scoping cost assume leveraging from a system implemented at another site.
4. Similar technology upgrades elsewhere have led to reductions in protective force of about 2.5 SPO III FTEs, which also proportionately reduces the staffing shortage overtime premium.

Option 2 - Facility Modifications

1. Facility modification costs with a contingency included are estimated at $6.1 million.
2. Based on reviews by the ProForce and security management, it was estimated that a 20 percent reduction in SPO IIIs (i.e., 16 FTE) could be achieved, with proportionate reductions in the staffing shortage overtime premium.

Option 3 - Underground Facility

1. Construction of the UGF with a contingency included is

Table 3: Option 2 - Facility Modifications (K)

Activity	FTE Req. (Months)	FTE Rate	Labor Cost	DS/DC	Total
Consulting and Department Support:[1]					
Protection Upgrade Delay Consulting	*4*	*$225*	$75	*$5*	$80
Recapture/Recovery Evaluation	*4*	*$225*	$75	*$5*	$80
Joint Tactical Simulation (JTS) Support	*3*	*$225*	$56		$56
Security Requirements & Planning Support	*3*	*$90*	$23		$23
Protective Force Support	*3*	*$83*	$21		$21
Reactor Operations Support	*3*	*$280*	$70		$70
Facility Modifications With Contingency[2]				***$6,100***	$6,100
PIDAS 1 Upgrade and Reconfiguration				*$750*	$750
Entry/Exit Control Modifications				*$250*	$250
Total			**$320**	**$7,110**	**$7,430**

Notes:

1. Department work for Option 1 is similar for Option 2.
2. Estimate combines internal and external contractor costs, and a contingency factor.

Added Annual Costs:	
Technical maintenance and quality testing	*$40*
Trouble shooting	*$10*
Pro Force training and performance testing	*$20*
Total Added Annual Costs	**$70**

Net Annual Savings:		
20% SPO III[a]	*16*	$992
Portion of staffing shortage		$496
PSAP savings		$0
Total Annual Savings		**$1,488**
Less Added Annual Costs		$70
Net Annual Savings		**$1,418**

Cost Analysis Over 10-yr Life of Upgraded Facility:	
Net Annual Savings	$1,418
Estimated Life of Upgraded Facility	10
Savings over Life of Upgraded Facility	$14,180
Less One-Time Costs	$7,430
Net Savings Over 10-yr Life	**$6,750**

Payback Period:	
One-Time Costs	$7,430
Net Annual Savings	$1,418
Payback Period (years)	**5.2**

Note a - A 20% reduction in SPO IIIs (i.e., 16 FTEs) was estimated by ProForce and Security Management

estimated at $10 million.

2. Actual savings for facilities similar to the UGF are reported as 50 percent of security staffing. The ProForce and security management estimate 50 percent reductions in SPO III and communicator levels and 1 FTE reduction for lieutenants.
3. Based on the reductions identified above, the staffing shortage overtime premium cost will be nearly eliminated except for 1 FTE at the lieutenant level. It is important to note that the purported reduction in SPO IIIs coincides with the ProForce's anticipated reduction caused by the physical "aging of the current personnel." The ProForce saw no difficulties meeting the 50 percent reduction if the UGF is completed in 2 years.

Table 4: Option 3 - Underground Facility (K)

Activity	FTE Req. (Months)	FTE Rate	Labor Cost	DS/DC	Total
Consulting and Department Support:[1]					
UGF Consulting	*6*	*$225*	$113		$113
Security Requirements & Planning Support	*3*	*$90*	$23		$23
Protective Force Support	*3*	*$83*	$21		$21
Reactor Operations Support	*3*	*$280*	$70		$70
Construct UGF With Contingency[2]				***$10,000***	$10,000
Decommission Old Facility[3]				***100***	100
Total			**$226**	**$10,100**	**$10,326**

Notes:
1. Department work for Options 1 and 2 is similar for Option 3.
2. Construction estimate combines internal and external contractor costs, and a contingency factor.
3. Costs will vary with the degree of decommissioning performed on the old facility.

Added Annual Costs:	
Technical maintenance and quality testing	$40
Trouble shooting[a]	$50
Pro Force training and performance testing	$25
ESS training	$25
Total Added Annual Costs	**$140**

Cost Analysis Over 10-yr Period of UGF:	
Net Annual Savings	$3,584
10-yr Period	10
Savings over 10-yr Period	$35,840
Less One-Time Costs	$10,326
Net Cost Savings Over 10 yrs	**$25,514**

Cost Analysis Over 30-yr Life of UGF:	
Net Annual Savings	$3,584
Estimated Life of UGF	30
Savings over Life of UGF	$107,520
Less One-Time Costs	$10,326
Net Cost Savings Over 30 yrs	**$97,194**

Net Annual Savings:		
ProForce:[b]		
50% SPO III	***39***	***$2,418***
50% Commun.	***6***	***$330***
Lieutenant	***1***	***$80***
Portion of staffing shortage[c]		***$877***
PSAP savings		***$9***
Annual PIDAS Maintenance		$10
Total Annual Savings		**$3,724**
Less Added Annual Costs		$140
Net Annual Savings		**$3,584**

Payback Period:	
One-Time Costs	$10,326
Net Annual Savings	$3,584
Payback Period (years)	**2.9**

Note:

a. Assumes 1/2 FTE down hole maintenance.

b. ProForce and Security Management estimate 50% reductions in SPO III and Communicator levels and 1 FTE at the Lieutenant level, as supported by similar UGF.

c. The reductions in SPO III and Lieutenant levels will nearly eliminate the staffing shortage overtime premium.

4. PSAP savings are based on actual reductions in ProForce staffing, using a rate of $500 per person. Options 1 and 2 do not present actual reductions in current levels of the ProForce because of the staffing shortage.

Quantitative Presentation of the Options

Spreadsheets for the options were available to examine the relationships closer and to provide opportunities for scenario analysis to be performed. The options are presented in Tables 1-4, with key assumptions described in the footnotes and noted as bold and italicized in the spreadsheets. Option 0 lists the estimated costs for fiscal year 200X. The baseline information is needed to identify projected relevant costs and relevant savings that differ for each option. For Options 1, 2, and 3, the investment costs are listed first. The added annual costs, annual savings, net annual savings, cost analysis over a 10-year period, and the payback period are presented after the investment cost. A comparison of the three

Table 5: Comparison of Options (K)

	Option 1 Technical Upgrades	**Option 2** Facility Modifications	**Option 3** Underground Facility
Investment Cost	**$2,490**	**$7,430**	**$10,326**
Net Annual Savings:			
Annual Savings	$233	$1,488	$3,724
Added Annual Costs	$70	$70	$140
Net Annual Savings	**$163**	**$1,418**	**$3,584**
Payback Period (yrs)	**15.3**	**5.2**	**2.9**
Expected Life (yrs)	**10**	**10**	**30**
Net Present Value, 8%, 10 yrs			
PV of net annual savings	$1,094	$9,515	$24,049
Investment	$2,490	$7,430	$10,326
Net Present Value	**<$1,396>**	**$2,085**	**$13,723**
Internal Rate of Return, 10 yrs	**<1%**	**14%**	**33%**
Key Assumptions:			
Investment Cost	$1,076 Vaults	$6,100 Modific.	$10,000 UGF
ProForce FTE Savings	$233, which is 2.5 SPO III	$1,488, which is 20% of SPO III	$3,714, which is 50% of SPO III, 50% of Commun., and 1 Lieutenant

options, that add net present value and internal rate of return, is found in Table 5.

Recommendations and Comments

Option 1 - Technology Upgrades does not generate significant cost savings to warrant investing in it. In fact, with the remaining life of 10 years for the research facility, Option 1 does not pay for itself.

Even though Option 2 - Facility Modifications generates a substantial amount of cost savings each year with a 20 percent reduction in SPO III, it requires $7.43 million, which is nearly three-fourths of the investment needed for Option 3 - UGF. Furthermore, the facility modifications are not intended to extend the remaining 10-year life of the research facility. Investing in Option 2 would simply delay making the important strategic decision of investing in an underground facility or outsourcing the nuclear research capability.

The cost analysis performed for the three options presented by security management clearly points to Option 3 — UGF as the best choice. While the underground facility would require the largest investment at $10,326,000, the net annual savings of $3,584,000 for the UGF far exceeds the expected savings of the other two options.

A common method within the DOE system to evaluate competing projects is the payback period. Since the three options all required two years to complete the construction/installation, the payback was computed from the time the facility would be operational. The payback period for Option 3 — UGF was 2.9 years, Option 2 — Facility Modifications was 5.2 years, and Option 3 — Technical Upgrades was 15.3 years. The expected life of the UGF would be 30 years in contrast to 10 years for the other two options. Clearly, the cost analysis supports Option 3 — UGF.

When discounted cash flow techniques were applied to the data over a 10-year period, the net present value of the projects using an 8 percent discount rate also supported Option 3 — UGF. Over the next ten years of the projects, Option 3 had a NPV of $13,723,000, Option 2 had $2,085,000, and Option 3 had <$1,396,000>. When an internal rate of return was computed over a 10-year period, Option 3 had an IRR of 33 percent, Option 2 an IRR of 14 percent, and Option 1 an IRR of less than 1 percent.

Option 3 - UGF represents a significant change in cost structure for security operations. The current total variable costs of the ProForce can be reduced significantly with an investment in new fixed costs of the UGF. The past has shown that each year, as protection standards increase and as the current facilities fall further behind in their ability to meet new standards, the costs for security operations everywhere in the DOE system continues to increase. The selection of Option 3 represents a strategic commitment to technology as a laboratory's innovative response to meeting protection standards at a lower cost. In addition, further opportunities will be available to a cost efficient research site, such as the transfer of current research projects and the obtainment of future research projects in the DOE system.

There is an obvious but important lesson that can be learned from the dilemma facing current nuclear research sites as it relates to security costs: the facilities built 30 years ago considered security issues as an afterthought, and it has been apparent now for years with escalating security costs. Security considerations must be an integral part of the design for a new facility, as evidenced by the cost savings associated with recently built underground facilities.

Dennis F. Togo is associate professor in the department of accounting at the University of New Mexico. He teaches cost and managerial accounting, and accounting information systems to undergraduate and graduate students. He has consulted with Sandia National Laboratories in its Safeguards and Security Division over the last five years. His work has focused on activity-based costing of security operations, cost estimation of protective force activities at nuclear research sites, relevant cost analysis of outsourcing decisions, and the cost analysis of facility upgrades. He is a graduate of Brigham Young University and Arizona State University with degrees in accounting and mathematics.

Claude S. Potter is a principle member of laboratory staff in the Security Requirements and Planning Department of Sandia National Laboratories. He has worked as a senior security analyst performing vulnerability analyses of special nuclear material protection systems and as project leader for cost analysis of security services and upgrades at nuclear material sites. His graduate degree is in business from the Anderson Schools of Management at the University of New Mexico.

Method and Setup for Measuring Trace Levels of Heavy Fissionable Elements Using Delayed Neutron Counting

V.M. Piksaikin, A.A. Goverdovski, G.M. Pshakin, and S.G. Isaev
Institute of Physics and Power Engineering, Obninsk, Russia

Abstract

After the unlimited extension of the Non-Proliferation Treaty in 1995 and approval by Member States Additional Protocol under the 93+2 Program, traditional safeguards approaches must be enhanced using new methods and techniques. One such method uses environmental sampling to trace undeclared activities such as enrichment and spent fuel reprocessing. This paper discusses methods for measuring trace levels of fissionable nuclides, using the delayed neutron counting technique. The electrostatic accelerator-based method uses the $^{9}Be(d,n)^{10}B$ reaction as a neutron source to determine ultra-trace levels (nano grams) of fissionable nuclides. In addition, a new method for determining sample isotopic content is proposed. This method is based on the systematic of the average half-life of delayed neutron precursors for different fissioning systems.

Introduction

The availability of a method for the identification of ultra-trace levels of fissionable elements (actinides) in samples of varied origins has many important applications. Commonly used methods of elemental analysis are neutron activation analysis, neutron-induced prompt gamma-ray analysis, and proton-induced X-ray analysis. The minimum detectable amounts are a function of many factors such as source strengths, detector efficiency, geometry, sample quality, interfering reactions, and other factors related to specific experiments. For instance, the reactor-based PGA method has the highest sensitivity, allowing thorium and uranium detection limits of approximately ~ 1 mg/g.[1] Currently, the more time-consuming alpha spectrometry method with preliminary actinide separation is routinely used for the identifying trace levels of these elements.

Elemental analysis using delayed neutron activity counting provides estimated minimum thorium and uranium detection levels of ~ 50 μg.[2] However the development of a more reliable database for DN parameters and utilization of high-strength neutron sources make it possible to extend the DN counting technique to ultra-trace level quantitative and qualitative analyses of fissionable elements.

Experimental Method/Setup for Fissionable Element Content Determination in Samples

The experimental setup was designed and successfully used for investigating delayed neutron yields from neutron induced fission of heavy nuclei.[3] The setup was installed at the electrostatic accelerator KG-2.5 with following parameters: ion (proton and deuteron) current — up to 500 μA, pneumatic sample delivery system — 150 ms and 1 s for 'fall down' sample delivery system, high voltage — up to 2 MV, neutron flux monitor — calibrated fission chamber, neutron detector - 30 boron counters embedded in the polyethylene moderator. Neutron detector efficiency is 0.084 with very low sensitivity to gamma-ray background of the sample under investigation. The intensity of the neutron background during delayed neutron counting period is about 0.008 counts/s per 1 μA of deuteron current in case of the (d, n) neutron production reactions.

The general equation for elemental analysis on the basis of the delayed neutron counting can be expressed as following

$$N(t_k) = A \cdot \sum_{i=1}^{i=m} F_i \cdot \frac{a_i}{\lambda_i} \cdot (1 - \exp(-\lambda_i \Delta t_k)) \cdot exp(-\lambda_i t_k) + B \cdot \Delta t_k \,, \quad (1)$$

$$F_i = (1 - exp(-\lambda_i t_{ir})) \left(\frac{n}{1 - \exp(-\lambda_i T) - exp(-\lambda_i T)} \left(\frac{1 - exp(-n\lambda_i T)}{((1 - \exp(-\lambda_i T))^2} \right) \right),$$

$$A = \varepsilon \, \sigma_f \varphi N_f \nu_d \,,$$

where $N(t_k)$ - the number of counts registered by the neutron detector in the time-channel t_k with time-channel width Δt_k, νd - the total delayed neutron yield per one fission, B- the intensity of neutron background, λ_i,a_i - the decay constant and relative abundance of i -th group of DN, n - the number of cycles, m- the number of DN groups, T - the duration of one cycle of measurements, which includes the irradiation and the delayed neutron counting time, t_{ir} - irradiation time, ε - efficiency of neutron detector, φ - the neutron flux, σf - fission cross section, Nf - the number of atoms of fissionable element (nuclide) under investigation.

Equation (1) and the value of parameters of the setup allow estimation of the (detectable concentration) detection limit of fis-

sionable elements (as well as minimal detectable amount) in the samples for the neutron source based on the $^{9}Be(d,n)^{10}B$ reaction and deuteron ion current of 500 μA [4] It was assumed that for the reliable analysis one needs to register 100 delayed neutron counts above the background. The result of the estimation for thorium, uranium and plutonium elements are presented in Table 1.

Table 1.
Sensitivity of Delayed Neutron Counting Technique for Analyzing Sample Content of Fissionable Elements

Nuclide	Minimal detectable amount *, g		Detectable concentration *, g/g	
	Fast neutron flux	Thermal neutron flux**	Fast neutron flux	Thermal neutron flux**
^{235}U	$6.3 \cdot 10^{-6}$	$1.5 \cdot 10^{-6}$	$1.3 \cdot 10^{-8}$	$3 \cdot 10^{-9}$
^{238}U	$1 \cdot 10^{-5}$		$2 \cdot 10^{-8}$	
^{239}Pu	$1 \cdot 10^{-5}$	$2.6 \cdot 10^{-6}$	$1.9 \cdot 10^{-8}$	$5 \cdot 10^{-9}$
^{232}Th	$1.7 \cdot 10^{-5}$		$3.3 \cdot 10^{-8}$	

* *Amounts which were obtained at the experimental conditions indicated in the text.*

** *Degradation of the neutron flux in the neutron slowing down process was taken into account.*

Ten cycles of irradiation and delayed neutron counting were taken into consideration. The sample irradiation time was 100 s and the delayed neutron counting time was 25 s starting at 1 s after the end of irradiation. The total time spent for analysis was 1,260 s. The estimation was made both for the fast neutron flux from the $^{9}Be(d,n)^{10}B$ reaction at 2 MeV deuteron energy and for the thermal neutron flux which can be easily obtained by slowing down the neutrons from the neutron target. Degradation of the neutron flux during the neutron slowing down process was accounted for.

It is seen from the Table 1 that the setup under discussion affords determination of trace levels of fissionable elements contained in the sample, using many cycles of measurements leads to increased analysis sensitivity. Moreover, in contrast to the gamma ray and alpha particle analysis methods, the delayed neutron counting method has no restriction on the weight of the sample under investigation. This fact leads to increasing the sensitivity of the analysis based on the delayed neutron counting. The detectable concentration of fissionable nuclides was estimated for 500g sample.

The combination of the fast neutron flux and the thermal neutron flux analysis allows the identification of the isotopic content of the sample.

Method of Sample Isotopic Content Identification

Until now the identification of isotopic content of the sample in the frame of the DN counting technique was based on the difference between the values of relative abundances of the definite DN group for different nuclides.[5] This method requires a high statistical accuracy of DN decay curve[6] and reliable data base for the DN group parameters (decay constants and relative abundances). But if one takes into account the strong correlations between DN group parameters originating from the least-squares fitting procedure of the decay curves[7] then it is difficult to rely on the reliable results on the determination of isotopic concentration in the frame of such method.

We propose another approach for the identification of isotopic content of samples which is based on the new systematic of the delayed neutron parameters.[8] According to this systematic the average half-life of the delayed neutron precursors for the isotopes of thorium, uranium, plutonium and americium elements can be presented by the following expression

$$\langle Ti\rangle = b_{1i} \cdot \exp\left[(b_{2i}(-(A_c - 3Z) \cdot A_c/Z\right], \quad (2)$$

where index i is related to the certain fissioning systems (thorium, uranium, etc.), A_c and Z - the mass number and atomic number of the fissioning nuclei respectively. The $-(A_c-3Z)(A_c/Z$ parameter is usually used for the systematics of the total DN yields. In general the Z2/Ac parameter can be taken as having the same scaling factor. The experimental data on the average half life parameters were obtained using the formula

$$\langle T\rangle = \sum_{i=1}^{6} a_i T_i,$$

where a_i and T_i are the relative abundance and period of the i-th DN group. The above expression (2) was presented in the form

$$\ln\langle T_i\rangle = b_{3i} + b_{2i}\left[-(A_c - 3Z) \cdot A_c/Z\right], \quad (3)$$
$$b_{3i} = lnb_{1i}$$

and the appropriate delayed neutron data were analyzed for obtaining the b_{3i} and b_{2i} values on the basis of the least-squares method. The results of the fitting procedure (solid lines) are shown in Figure 1. The obtained b_{3i} and b_{2i} values for each of the considered element are presented in Table 2. Thus all of the known isotopes can uniquely be identified by only one parameter — the average half-life of the delayed neutron precursors. Therefore, for the identification of the isotopic content of the sample one needs to make measurements using the least squares

Table 2.
Results of LSM Analysis of DN Experimental Data

Element	b_3	b_2, ($\times 10^2$)
Th	-10.55 ± 0.48	13.05 ± 0.50
U	- 5.36 ± 0.29	7.34 ± 0.28
Pu	- 4.44 ± 0.61	6.32 ± 0.57
Am	- 2.78 ± 1.08	4.73 ± 0.99

analysis of DN decay curve with the purpose of obtaining the value of the average half-life parameter (for the mixture of nuclides).

In cases where two nuclides are present in the sample, the obtained value $\langle T_{1,2}\rangle$ is connected to unknown value of the fractional amount of the number of atoms of nuclides 1 and 2 by the following expressions

$$\langle T_{1,2}\rangle = (\nu_1\sigma_1\varphi m_1\langle T_1\rangle + \nu_2\sigma_2\varphi m_2\langle T_1\rangle/(\nu_1\sigma_1\varphi m_1 + \nu_2\sigma_2\varphi m_2),$$
$$m_1 + m_2 = 1,$$

where ν_1, ν_2 — the total delayed neutron yields related to nuclide 1 and 2, σ_1, σ_2 — the fission cross section of nuclides 1 and 2, $\langle T_1\rangle$, $\langle T_2\rangle$ — the average half-life of DN precursors of nuclide 1 and 2, m_1, m_2 — the fractional amount of the number of atoms of nuclide 1 and 2 respectively, φ — the neutron flux through the sample.

In cases where three nuclides are present in the sample, with two of them fissionable by thermal neutrons (for example ^{235}U, ^{238}U, ^{239}Pu), the combination of the fast neutron and thermal neutron flux analysis will give the average half-life values $\langle T_{12}\rangle$ and $\langle T_{123}\rangle$ respectively, for the mixture of nuclides which are connected to the fractional amount of the number of atoms of nuclides m_1, m_2 , and m_3 in the sample by the following expression

$$\langle T_{1,2}\rangle=(\nu_1\sigma_{1,th}\varphi_{th}m_1\langle T_1\rangle+\nu_2\sigma_{2,th}\varphi_{th}m_2\langle T_{1,2}\rangle)/$$
$$(\nu_1\sigma_{1,th}\varphi_{th}m_1+\nu_2\sigma_{2,th}\varphi_{th}m_2),$$

$$\langle T_{1,2,3}\rangle=(\nu_1\sigma_{1f}\varphi_f m_1\langle T_1\rangle+\nu_2\sigma_{2f}\varphi_f m2\langle T_2\rangle+\nu_3\sigma_{3f}\varphi_f m_3\langle T_3\rangle)/$$
$$/(\nu_1\sigma_{1f}\varphi_f m_1+\nu_2\sigma_{2f}\varphi_f m_2+\nu_3\sigma_{3f}\varphi_f m_3)$$

$$m_1 + m_2 + m_3 = 1,$$

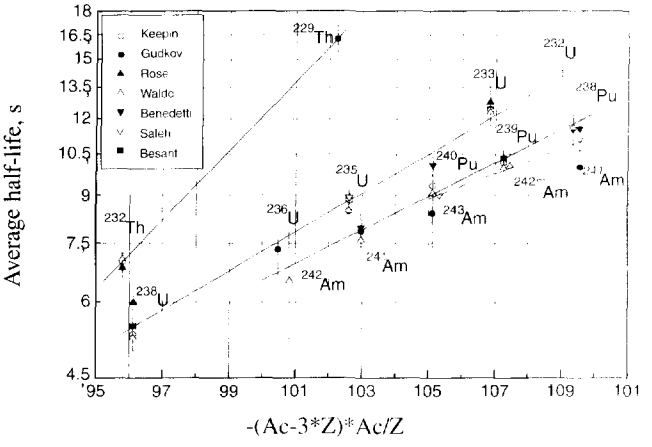
where $\sigma_{1,th}$, σ_{1f} and φ_{th} , φ_f — are the fission cross sections and the neutron fluxes for thermal and fast neutrons respectively. $\langle T\rangle$ values for thermal and fast neutron induced fission of all fissioning system were assumed to be equal.

It is necessary to note that the proposed method for isotopic determination in the present formulation assumes the high statistical accuracy of the measured decay curves that allows obtaining the reliable data on the average half-life values. This condition imposes the certain restriction on the weight of the fissionable samples.

Measurements of Isotopic Content of Sample Containing ^{235}U and ^{239}Pu

The discussed method was applied for the determination of isotopic content in the sample containing a mixture of ^{235}U and ^{239}Pu. The sample was irradiated by thermal neutrons with following measurements of delayed neutron decay curve. Twelve cycles of irradiation and delayed neutron counting were made. Each cycle includes the irradiation time of 300 s and the 724.5 s interval for DN counting. The sample delivery time from the irradiation position to the detector was about 0.15 s. The "thermal"-neutron spectrum was obtained within a 20-cm cubic polyethylene block, cadmium shielded and mounted at the accelerator neutron source based on the T(p,n)^{3}He reaction. The fission reaction rates $\langle\sigma\cdot\varphi\rangle$ averaged over the sample at the irradiation position for isotopes ^{235}U and ^{239}Pu were obtained on the basis of Monte Carlo calculations. The relative abundances and periods of delayed neutrons for the mixture sample were obtained in the analysis of decay curve by the iteration least-square method [3]. The values of the delayed neutron relative abundances and periods for thermal neutron induced fission of ^{235}U and ^{239}Pu were obtained in the analysis of decay curves measured in the independent experiment. On the basis of the measured data the values of average half-life of delayed neutron precursors

Fig. 1 Systematics of the average half-life of delayed neutron precursors.



$$\langle T\rangle = \sum_{i=1}^{6} a_i \cdot T_i$$

were obtained for each component ($\langle T\rangle_{235}$ and $\langle T\rangle_{239}$) of the sample and for their mixture ($\langle T\rangle_{mix}$). The fractional amounts of the number of the ^{235}U and ^{239}Pu atoms were calculated using the following formulas

$$m^{235} = \frac{A^{rel}_{235}/\nu\cdot\langle\sigma\cdot\varphi\rangle_{239}}{A^{rel}_{235}/(\nu\cdot\langle\sigma\cdot\varphi\rangle_{235} + A^{rel}_{239}/(\nu\cdot\langle\sigma\cdot\varphi\rangle_{239}}$$

$$m^{239} = \frac{A^{rel}_{239}/(\nu\cdot\langle\sigma\cdot\varphi\rangle_{235}}{A^{rel}_{235}/(\nu\cdot\langle\sigma\cdot\varphi\rangle_{235} + A^{rel}_{239}/(\nu\cdot\langle\sigma\cdot\varphi\rangle_{239}}$$

$$A^{rel}_{235} = \frac{\langle T\rangle_{mix} - \langle T\rangle_{239}}{\langle T\rangle_{239} - \langle T\rangle_{235}}, \quad A^{rel}_{239} = \frac{\langle T\rangle_{mix} - \langle T\rangle_{235}}{\langle T\rangle_{239} - \langle T\rangle_{235}}$$

(4)

It is necessary to note that in the present work the fractional amounts of the number of ^{235}U and ^{239}Pu nuclei were obtained in addition by another technique that is based on the least-squares method analysis of the DN decay curves. The DN decay

curves measured after irradiation of ^{235}U, ^{239}Pu and a mixture sample were simultaneously analyzed with the purpose to obtain the values of the relative saturation activity for each component under investigation (A^{rel}_{235} and A^{rel}_{239}). The fractional amounts of the number of ^{235}U and ^{239}Pu atoms were calculated using equation (4).

The known and experimental values of the fractional amounts of the number of ^{235}U and ^{239}Pu nuclei obtained by two methods are presented in Table 3. The values of the total delayed neutron yields and the fission rate values that were used in the calculations also are presented in Table 3.

Table 3.
Experimental Results of the Fractional Amounts of the Number of ^{235}U and ^{239}Pu Nuclei

Input data and results	Isotope	
	^{235}U	^{239}Pu
ν, %	1.621±0.056	0.628±0.038
$(\sigma\cdot\varphi)10^{-7}$, s^{-1}	2.65889	1.81563
A^{rel} (obtained using <T>)	0.6785±0.0876	0.3215±0.0876
m, % (obtained using <T>)	35.82±7.11	64.18±7.11
A^{rel} (obtained by LSM)	0.7088±0.0683	0.2912±0.0683
m, % (obtained by LSM)	39.17±6.27	60.83±6.27
m, % (known)	39.02±0.39	60.98±0.61

From Table 3 one can see that the experimental and known values of the fractional amounts agree within the quoted uncertainties. It is necessary to note that in the present work only one measurement of the fractional amounts was done. One way to increase the accuracy of the measurements by the present methods is to increase the number of measurements of the fractional amount.

In general the values of uncertainties depend on the ratio of the average half-lives of the isotopes under consideration. For instance in the case of ^{235}U and ^{238}U mixture the value of fractional amount uncertainties of 3-4 % can be obtained.

Conclusion

The DN counting technique, coupled with the electrostatic accelerator-based neutron source $^{9}Be(d,n)^{10}B$, is a powerful instrument in analyzing trace levels of fissionable elements in the samples of varied origins. The combination of thermal and fast neutron measurements and the analysis of the appropriate aggregate decay curves, with the purpose of obtaining the average half-life parameters, extends the possibilities of the techniques to the identification of the isotopic abundances in the sample under investigation.

This work was made under the Russian Foundation for Basic Research, grant No. 96-02-17439.

References

1. Chrien, Neutron radiative capture. *Neutron Physics and Nuclear Data in Science and Technology,* v.3, OECD/NEA, Pergamon Press, 1984.
2. J.W. McKlveen, "Fast Neutron Activation Analysis." (Elemental data base). Ann Arbor Science Publishers, Inc., 1981.
3. V.M. Piksaikin, Yu.F. Balakshev, et al. "Measurements of Periods," Relative Abundances and Absolute Total Yields of Delayed Neutrons from Fast Neutron Induced Fission of ^{237}Np. Proceedings of the International Conference on Nuclear Data for Science and Technology, Trieste, Italy, May, 1997.
4. N.A. Lose. "Nuclear Data for Industrial Neutron Sources. Proceedings of the International Conference on Nuclear Data for Science and Technology," Julich, May 1991, p.678-680.
5. B.P. Maksjutenko, Yu.F. Balakshev, et al. "Determination of Percentage Content of ^{235}U and ^{239}Pu Mixture Using Delayed Neutrons," *Atomic Energy* (in Russian), 1975, V. 39, No. 6, p. 420-422.
6. G.R. Keepin. *Physics of Nuclear Kinetics,* Addison-Wesley Pub. Co., 1965.
7. R. J. Tuttle. "Delayed-Neutron Data for Reactor-Physics Analysis," *Nuclear Science and Engineering,* 56, 1975, p.37.
8. V.M. Piksaikin, S.G. Isaev. Correlation Properties of Delayed Neutrons from Fast Neutron Induced Fission. Report INDC(CCP)-415, IAEA, Vienna, 1998.

INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT INMM ESARDA

INMM/ESARDA Third Workshop on Science and Modern Technology for Safeguards

November 13–16, 2000
International House of Japan
Tokyo

In order to promote improvements in International Safeguards through the incorporation and use of results from science and advanced technology development, and to encourage the advancement of nuclear materials management, INMM and ESARDA are jointly sponsoring the Third Workshop on Science and Modern Technology for Safeguards. The goals of the workshop are:

- to inform the safeguards community about current research in the natural and social sciences, and about selected, advanced technologies that could be used to support needed advances in international safeguards, and that will become available for use in the next few years, and
- to stimulate application of such science and advanced technology to safeguards by providing an opportunity for technical interchange between researchers and safeguards experts.

As was the case for the previous workshops, this third workshop will have four working groups. The topics to be considered in these working groups are:

- Regional Systems and State Systems of Accounting and Control
- Social-Political Aspects of Safeguards
- Safeguards Challenges of Future Energy Technologies, and
- Automation, Robotics, and Expert Software.

Registration materials will be available after August 1, 2000, and may be obtained by contacting INMM Headquarters or by accessing INMM's Web site.

Institute of Nuclear Materials Management
60 Revere Drive, Suite 500
Northbrook, IL 60062
847/480-9573
Fax: 847/480-9282
E-mail: inmm@inmm.org
www.inmm.org

Registration fee: $125 U.S.

Sponsored by the Institute of Nuclear Materials Management's International Safeguards Division, and the European Safeguards Research and Development Association. Hosted by the Japan and Korea Chapters INMM.

INMM 41ST ANNUAL MEETING

Hilton New Orleans
Riverside Hotel
July 16-20, 2000
New Orleans, Louisiana

INMM
INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT

For more information please contact
INMM Headquarters at 847/480-9573

June 4–8
ANS Annual Meeting, San Diego, California. Sponsor: American Nuclear Society. Contact: ANS phone, 708/352-6611, fax, 708/ 352-0499; Web site, http://www. ans.org.

June 5–6
Emergency Planning Information Forum, The Abbey Resort on Lake Geneva, Fontana, Wisconsin, U.S.A. Sponsor: Nuclear Energy Institute. Contact Kim Shear, NEI; phone, 202/739-8028.

June 12–16
4th U.S. Department of Energy International Decommissioning Symposium, Knoxville Convention Center, Knoxville, Tennessee. Sponsor: U.S. Department of Energy. Contact: Call 305/348-3752; E-mail, elaine@eng.fiu. edu, or write IDS 2000. Florida International University, Hemispheric Center for Environmental Technology, 10555 W. Flagler St., Suite 2100, Miami, Florida 33174.

June 19–21
World Engineers' Convention 2000. Hanover, Germany. Sponsors: VDI The Association of Engineers and Expo 2000 Hanover. Contact: VDI The Association of Engineers, P.O. Box 10 11 39, D-40002 Duesseldorf, Germany; call +49 221 6214-440; fax +49 211 6214-167; E-mail, tagungen@vdi.de; Web site, http://www.vdi.de/wec/.

June 19–21
U.S. Women in Nuclear National Workshop, The Desert Inn, Las Vegas, Nevada, U.S.A. Sponsor: Nuclear Energy Institute. Contact: Linda Hertzog, NEI; phone, 202/739-8014.

June 21–22
ASTM Committee F23 on Protective Clothing, Sheraton Hotel, Toronto, Canada. Sponor: ASTM. Contact: Steve Mawn, 610/832-9726; E-mail, smawn@astm.org.

July 16–20
41st INMM Annual Meeting, The Hilton Riverside New Orleans, New Orleans, Louisiana. Sponsor: Institute of Nuclear Materials Management. Contact: INMM; phone, 847/480-9573; fax, 847/480-9282; E-mail, inmm@inmm.org; Web site: http://www.inmm.org.

July 26
Nuclear Fuel Supply Forum, Willard Inter-Continental Hotel, Washington, D.C., U.S.A. Sponsor: Nuclear Energy Institute. Contact: Conference Office; phone, 202/739-8000; fax, 202/872-0560.

August 30–September 10
25th Annual Symposium of the Uranium Institute, London, U.K. Sponsor: Uranium Institute. Contact: UI; phone 0171 225 0303; E-mail, ui@uilondon.org.

September 18–20
4th Conference on AeroSpace Materials, Processes, and Environmental Technology (Formerly the Aerospace Technology Conference), Von Braun Center, Huntsville, Alabama. Sponsors: Marshall Space Flight Center, NASA Operational Environment Team, NASA's Materials and Processes Working Group, Office of Space Flight, NASA Headquarters, National Center for Advanced Manufacturing, American Institute of Aeronautics and Astronautics, American Society of Metal International®, Aerospace Industries Association, Environmental Protection Agency, National Center for Manufacturing Services, Sandia National Laboratories, Society for Advancement of Materials and Process Engineering, and the University of New Orleans. Contact: Jodi Weiner; phone, 256/533-5923; fax, 256/534-9899; E-mail: jweiner@ aol.com, Web site, http://ampet.msfc.nasa.gov.

September 24-27
NEI International Uranium Fuel Seminar 2000, Resort at Squaw Creek, Olympia Valley, California, U.S.A. Sponsor: Nuclear Energy Institute. Contact: Nicki Rocco, NEI; phone, 202/739-8014.

October 22-25
Communicating Nuclear Issues, Wyndam Cleveland Hotel, Cleveland, Ohio, U.S.A. Sponsor: Nuclear Energy Institute. Contact: Linda Hertzog, NEI; phone, 202/739-8026.

November 13–16
Third Workshop on Science and Modern Technology for Safeguards, Tokyo, Japan. Sponsored by INMM and ESARDA. Registration materials will be available after Aug. 1, 2000. Contact: INMM, 60 Revere Drive, Suite 500, Northbrook, IL 60062 U.S.A. phone, 847/480-957, fax, 847/480-9282; E-mail, inmm@inmm.org.

June 10-14, 2001
ASTM 13th International Symposium on Zirconium in the Nuclear Industry, Annecy, France. Sponsor: ASTM Committee B-10 on Reactive and Refractory Metals and Alloys. Contact: Gerry Moan, AECL, 2251 Speakman Drive, Mississauga, Ontario, Canada L5K 1B2; 905/823-9060, Ext. 3232; E-mail: moang@aecl.ca.

September 3-7, 2001
PATRAM 2001, Chicago, Ill., U.S.A. Sponsors: US Department of Energy, in cooperation with the International Atomic Energy Agency. Hosted by the Institute for Nuclear Materials Management. Chicago Hilton and Towers. Contact: INMM, 847/480-9573; E-mail: inmm@inmm.org.