JNMM
Journal of Nuclear
Materials Management

Published by the Institute of Nuclear Materials Management ■ Volume XXVIII, Number 4 ■ Summer 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*
Shunji 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, *Administrative Director*
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.

CONTENTS

Volume XXVIII, Number 4 • Summer 2000

PAPERS

EDITORIALS

INMM NEWS

ANNOUNCEMENTS

The INMM Challenge

Each year the INMM faces the challenge of offering greater value to the members and community-at-large. We sponsor an increasing number of activities each year, including the Annual Meeting, technical workshops, and chapter events. We could expand these initiatives and tackle new ones if we could find a few more energetic professionals like you to volunteer their time.

The 41st Annual Meeting of the INMM July 16-20, 2000, in New Orleans, Louisiana, will demonstrate firsthand the positive results of our efforts this past year. I would like to encourage you to find a way to become more involved in INMM activities and help the organization grow even stronger.

Consider writing articles for the *Journal*, serving on technical divisions and committees, assisting at the annual meeting and workshops, participating in local chapter activities.

Several years ago, the INMM reorganized in order to reflect more effectively the issues, technologies, and capabilities needed to assist in the implementation of international nuclear materials management and nonproliferation objectives. This reorganization is reflected in the following list of technical divisions and their chairs:

- Nonproliferation and Arms Control
  Chair: C. Ruth Kempf,
  516/344-7226
- Physical Protection
  Chair: Steve Ortiz
  505/845-8098
- Materials Control and Accountability
  Chair: Dennis Brandt
  505/667-0645
- Packaging and Transportation
  Chair: Bill Cole
  202/479-2116
- Waste Management
  Chair: Ed Johnson
  703/359-0842
- International Safeguards
  Chair: Cecil Sonnier
  505/298-1248

In addition to the technical divisions, there are a number of standing committees that are also serve important roles in the Institute. These committees include:

- Annual Meeting Oversight
  J.D. Williams
  505/845-8766
- Technical Program Committee
  Charles Pietri
  708/246-8489
- Exhibits
  Ken Ystesund
  505/844-6067
- Registration
  Chris Hodge
  925/443-1983
- Bylaws and Constitution
  Roy Cardwell
  423/986-7347
- Awards
  Yvonne Ferris
  301/903-6619
- Fellows
  Obie Amacker
  509/376-1330
- Communications
  Cathy Key
  825/576-6902
- Government/Industry Liaison
  James R. Lemley
  516/344-2916
  Amy B. Whitworth
  202/586-8538
- Membership
  Nancy Jo Nicholas
  505/667-1194

The INMM also serves as the secretariat for two ANSI standards. The INMM chairs for these two committees are:

- N.14
  John Arendt
  423/483-1401
- N.15
  Joe Rivers
  301/353-0172

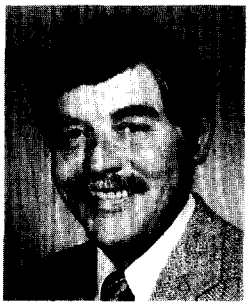
In addition, the *JNMM* itself has a number of volunteers who serve as editors, oversee production and editing, and write articles. Denny Mangan is the technical editor of the *JNMM*, and he has a number of associate editors who help make the *JNMM* an excellent publication. If you are interested in working on the *JNMM*, please contact Denny at Sandia National Laboratories. (See Technical Editor's Note, page 3.)

These are just a few of the dedicated people who volunteer their time to serve the INMM. I'm sure that no matter what your talents are, or how limited your time is, we have a way you can help the INMM. Please consider using your time and energy time to help make INMM a stronger organization for everyone.

As always, I welcome your comments and look forward to seeing you in New Orleans.

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

Spent Fuel Seminar Provides Food for Thought



In this issue of the *Journal*, we feature two articles that were presented at the INMM's 17th annual Spent Fuel Management Seminar last January in Washington, D.C. They were recommended by Ed Johnson, chair of the INMM Waste Management Technical Division, and his colleagues. We hope to publish three more recommended papers in the near future.

This issue of the *Journal* begins with a paper titled, Remote Monitoring Architectures: A Part of the Frontier, by Phillip Campbell, Richard Craft, and Lillian Snyder, all from Sandia National Laboratories. They discuss various architectures that can be used in remote monitoring and discuss issues that need to be addressed. They conclude with discussions on different types of architectures being planned for use in various applications.

In the second paper, William Stanbro and Kory Budlong-Sylvester of Los Alamos National Laboratory discuss the possibility of using expert judgment in safeguards. In their paper, "The Role of Expert Judgment in Safeguards," they review the use of expert judgement in forensics, medicine, environmental management, and nuclear safety. They then postulate how expert elicitation might be used in safeguards. It's interesting reading.

In his paper, Physical Protection Performance Testing: Assessing U.S. NRC Experience, Oleg Bukharin of Princeton University provides a fairly comprehensive review of the way the Nuclear Regulatory Commission assesses the performance of physical protection systems. I can personally recall the days when the NRC gave consideration to performance versus prescriptive evaluations. Bukharin's paper brought back many memories.

The paper, IAEA's Transportation Burnup Credit Activities, by William Lake of the U.S. Department of Energy, and H. Peter Dyck of the International Atomic Energy Agency, is one of the papers recommended by Ed Johnson for publication. I found it fascinating reading. I had no idea of what was meant by transportation burnup credit, nor the value of considering it. I hope you also enjoy this paper.

The final paper in this issue was also recommended by Ed Johnson. Written by F. Takats of TS ENERCON KFT in Budapest, Hungary, and H. Peter Dyck of the International Atomic Energy Agency, it reviews the spent fuel management approaches in thirteen different countries. For one reason or another, spent fuel seems to be on the rise.

As you may know, the *Journal* has undergone a change in staff at INMM Headquarters. Patricia Sullivan is now the managing editor at Headquarters, and is rapidly becoming familiar with our profession. She has worked hard to get the *Journal* back on schedule, for which she should be commended. Hopefully the rough part in the transition is over and the publications will become more timely. She will be attending the Annual Meeting, so please take the opportunity to discuss the *Journal* with her.

As always, I welcome any comments or suggestions you may have. I also 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, NM, U.S.A.
Phone: 505/845-8710
Fax: 505/844-6067
E-mail: dlmanga@sandia.gov

Relief Fund for Los Alamos Employees Accepting Donations

A relief fund has been set up to benefit the federal and contractor employees at Los Alamos Area Office and contractor employees at Los Alamos National Laboratory who were victims of the wild fire that destroyed so much of Los Alamos, New Mexico, this spring.

The Northern New Mexico Fire Recovery Fund was established by U.S. Secretary of Energy Bill Richardson in May while the fire was still raging. Public and private donations are being accepted. Donations are tax deductible.

The DOE's Los Alamos Area Office employs 65 people while LANL employs 8,000.

Donations can be mailed to:
U.S. Department of Energy
Attn: Northern New Mexico Fire Recovery Fund
Office of Chief Financial Officer, CR-52
P.O. Box 500
Germantown, MD 20874-0500

No Imminent Risk at DOE Nuclear Sites

An assessment of key Energy Department sites around the United States concludes that there is no imminent risk of a nuclear accident at the department's nuclear sites. It also recommends that steps be taken to improve nuclear safety programs and the professional expertise of those responsible for implementing nuclear safety precautions. The study was initiated at the direction of President Clinton after the September 1999 nuclear accident in Japan.

The report, "Nuclear Criticality Safety at Key Department of Energy Facilities," assesses the risk of an unplanned nuclear reaction—or nuclear criticality accident—at major sites in the department's nuclear weapons complex. The study finds that the risk of an accident similar to the one in Japan does not exist in the U.S. primarily because the Energy Department has adopted and adheres to national standards for operations and training specifically designed to reduce the risk of these types of accidents.

The report focussed on the department's Los Alamos National Laboratory in New Mexico, Rocky Flats Environmental Technology Site outside Denver, Colo., Hanford Site, in Washington state, Savannah River Site in South Carolina, and Y-12 Plant in Oak Ridge, Tennessee.

The report identifies two general areas for improvement at DOE headquarters and three general areas for improvement at its sites. It recommends headquarters revise DOE orders and guidance to remove inconsistencies with national industry standards and strengthen nuclear criticality safety programs at sites. The report also recommends that all sites assess their safety programs and take any steps needed to ensure operators understand the controls and technical bases designed to prevent criticality accidents; ensure strict adherence to procedures and controls; and improve the processes for feedback and improvement.

A copy of the report is available at http://www.eh.doe.gov.

Taskforce Created to Study Nonproliferation Programs in Russia

U.S. Secretary of Energy Bill Richardson appointed a blue-ribbon panel to review and assess the Energy Department's nonproliferation programs in Russia and recommend how its nonproliferation efforts can be enhanced. Former White House Counsel Lloyd Cutler and former Senate Majority Leader Howard Baker will serve as co-chairmen of the panel.

The taskforce will assess DOE's ongoing nonproliferation activities with Russia and will provide policy recommendations on how to support effectively U.S. national security interests. The assessment will include but not be limited to:

- Initiatives for the Proliferation Prevention Program;
- The Nuclear Cities Initiative;
- The Material Protection Control and Accounting Program;
- The Second Line of Defense Program;
- The HEU Purchase Agreement;
- The International Nuclear Safety Program; and
- The Plutonium Disposition Program.

The taskforce held its first meeting March 13.

ASTM Standardization News Magazine Now Online

ASTM *Standardization News* magazine, one of the premier publications in the world covering standards development, is now online at http://www.astm.org.

Standardization News is the official publication of ASTM, one of the largest voluntary standards development systems in the world. In addition to featuring ASTM technical committee standards development activities, the magazine publishes news about national and global standards activities.

BNFL Awarded Contract for Waste Assay Systems in Japan

BNFL Instruments has won a multi-million pound contract to supply crate and drum monitors to Japan Nuclear Fuel Ltd., for use at the Rokkasho Reprocessing Plant which is being built by JNFL in Aomori prefecture, Japan.

Two crate monitors and one drum monitor will be installed and commissioned in the plant, the first full scale facility of its kind in Japan. The plant will reprocess fuels from light water nuclear reactors.

The specially designed monitors will be used to measure and characterize the plutonium content of waste packages in large crates weighing up to 4,000 kg and

also 200-liter drums, providing data that will assist JNFL in satisfying international safeguards regulatory requirements.

The waste assay systems are based on a unique physics design devloped specifically for this project by Los Alamos National Laboratory. This will be the largest of a series of ventures where LANL and BNFL have worked together.

EKOR Being Applied at Chernobyl

Workers at the Ukraine's Chernobyl nuclear power plant in March began coating the sarcophagus encasing a destroyed reactor with a special material designed to protect the nuclear waste inside from exposure to the environment, according to a statement released by the company that produces the product. A spokesman for EuroTech Ltd., producer of EKOR, said the product thickens and hermetically seals the waste inside for up to 300 years.

EuroTech conducted demonstrations of its product in late April for U.S. Department of Energy officials at the Hanford Site in Richland, Washington.

Los Alamos TA-18 to Close

The U.S. Department of Energy will close Technical Area 18 at its Los Alamos National Laboratory by the end of 2004, according to a statement released by the DOE in April. An environmental impact study on the proposed transfer of TA-18's capabilities and materials to another locale will be completed in December 2000. The facility supports defense, nuclear safety, and national security missions.

Though TA-18 is judged safe and secure by the DOE's independent inspection office, its facilities are 30 to 50 years old and are increasingly expensive to operate and maintain. Another Los Alamos site is the preferred relocation option, but other DOE facilities, including the Nevada Test Site and Argonne-West in Idaho, will be considered.

About 80 people work full-time at TA-18. They provide expertise and knowledge in advanced nuclear technologies that support critical experiments in Stockpile Stewardship and nuclear safety programs throughout the DOE; emergency response in support of counterterrorism activities; and safeguards and arms control in support of domestic and international programs to control nuclear materials.

DOE Makes New Commitments for Hanford Cleanup

In May, U.S. Secretary of Energy Bill Richardson announced new commitments to the state of Washington to clean up the Hanford tanks in Richland, Washington. The five-part commitment to the state includes provisions that assure that:

- The department and state will immediately amend the existing consent decree to include two new milestones. By August 2000, DOE will issue a Request for Proposals for a new design and construction contract asking for proposals that will allow DOE to meet 2007 milestones under the Tri-Party Agreement. By Jan. 15, 2001, the DOE will award a contract.
- Over the next 15 months, the DOE and Washington will try to negotiate a new consent decree establishing more commitments aligned to the new contract.
- The DOE will unilaterally commit to no shipments of waste to Hanford from new sources while the DOE works to get the new contract on firm footing.
- The state and DOE will continue to discuss longer term commitments regarding the shipment of waste into the state.
- The department and the state have agreed to engage the U.S. Environmental Protection Agency in a discussion about how to realign cleanup commitments for the entire Hanford site to ensure that the goals are achievable and to address the most important problems first.

New Members

Trevor Robert Barrett
Barrot Assessment Consulting Ltd.
16 Rockwell Crescent
Thurso Caithness KW14 7PL
United Kingdom
01847-89-3304
Fax: 01847-89-1712
E-mail: trevor.barrett@ukgateway.net

Paul J. Bartak
Honeywell FM&T
P.O. Box 419159
Kansas City, MO 64141-6159
816/997-2467

Terry F. Hannon
Bechtel Jacobs Company L.L.C.
111 Dewey Road
Oak Ridge, TN 37830
865/574-8985
E-mail: zth@bechteljacobs.org

Robert D. MacDougall
Numark Associates, Inc.
1150 Connecticut Ave., NW
Suite 715
Washington, D.C. 20036
202/466-2700
Fax: 202/466-3669
E-mail: rdmacdougall@numarkassoc.com

Ole Christen Reistad
865 17 Mile Drive
Pacific Grove, CA 93950
831/333-1887
E-mail: ole.reistad@miis.edu

Bret E. Simpkins
Battelle
902 Battelle Blvd.
P.O. Box 999
Richland, WA 99352
509/372-4601
Fax: 509/372-4316
E-mail: bret.simpkins@pnl.gov

Vaughn Standley
IAEA
P.O. Box 200
Vienna A-1400
Austria
43-1-2600-26313
E-mail: v.standley@iaea.org

Karen Wright
U.S. Department of Energy
1000 Indpendence Ave., SW
NN-44, GA-033, 6-8460
Washington, D.C. 20585
202/586-5742
Fax: 202/586-0936
E-mail: karen.wright@hq.doe.gov

Hui Zhang
Harvard University
BCSIA, Kennedy School of Government
79 JFK St.
Cambridge, MA 2138
617/496-2352
Fax: 617/496-0606
E-mail: hui_zhang@harvard.edu

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.

Remote Monitoring Architectures: A Part of the Frontier

Philip L. Campbell, Richard L. Craft, and Lillian A. Snyder
Sandia National Laboratories
Albuquerque, New Mexico, U.S.A.

Abstract

This paper presents a taxonomy, in the form of an abstract model, of the set of remote monitoring architectures, such as those used for international agreements, treaties, or the monitoring of hazardous materials. The model consists of three parts: a sensor, an optional server, and a user, with communication lines connecting sensor and server and connecting server and user. (If the server is not present, then the communication line connects the sensor and user directly.) We refine the three parts to include different user populations, data sensitivity, and secure services. We complete the model by allowing data between the parts to be either pulled or pushed. This results in six basic partitions, each of which has a number of sub-partitions. For several sample architectures we show how they fit into the taxonomy. The importance of the taxonomy is that it provides a systematic method of understanding these architectures which we believe are on the forefront of technology. We anticipate that solutions generated by these architectures will become commonplace in the future. For example, a customary requirement for these architectures is that the adversary be a legitimate user.

Background

Remote monitoring architectures operate in a high-risk environment. The first aspect of that environment that contributes to the risk is that the designer does not have complete control. A second aspect is that the adversary may be a legitimate user. A third aspect is that the data is of high consequence, the stuff of which wars are made, for example. These architectures are not designed for high-connectivity. However, the problems that they must address puts them in a position to provide solutions to networks that continue to push for more connectivity. Higher connectivity inevitably involves less control, more access by rogue users, and data of higher consequence. The last item follows inevitably only because of the nature of users: if the connection is already there and if it is already good enough for data of security level n, then please make it good enough for data of security level n+1.

Remote monitoring architectures have been of interest to the nuclear weapons community in general, and Sandia National Laboratories in particular, for several decades. One application of special interest to Sandia has been the development of a treaty verification system involving two adversarial parties, a host and a monitor, in which the host allows the monitor to place seismometers on its (the host's) soil. The monitor requires a guarantee that it receive all of the seismic data. The host on the other hand requires two guarantees: (1) that only the monitor receive the data, and (2) that the data that the monitor receives is limited to seismic data. That is, the host requires that there be neither eavesdropping nor covert channels. When the requirements demanded by the monitor and host are combined, they appear to be mutually exclusive and irreconcilable.

A compromise solution was developed in the early 1970s: a digital data authenticator as it was called then, or a message authenticating code, or MAC, as it would be called today. The scheme works as follows: As raw data is generated by the sensor, a MAC, consisting of a unique message identifier such as a message number, is attached. The host can view the data after it is generated but before it is sent to the monitor. The host then encrypts both the raw data and the associated MAC using a symmetric key encryption algorithm—the only kind available at that time—and sends the message along to the monitor. This scheme satisfies all of the requirements except for the host's stipulation that covert channels be eliminated. It is possible for the monitor to insert a covert channel in the MAC. If the host has the key upon which the MAC is based, then the host can eliminate covert channels, but then the host can also cheat by changing the raw data and generating a matching MAC. However, if the host does not have the key, then the host cannot verify that the proposed MAC matches what an untainted version of the algorithm would generate. The host demands the key, but the monitor demands that it not be given.

This problem was addressed by the advent of asymmetric encryption systems. Using asymmetric encryption, the host can verify the MAC without being able to produce a legitimate one. Asymmetric encryption also enables additional services: it gives both parties the ability to convince a third-party of the other's non-compliance and/or their own compliance via what is known as non-repudiation.[1] As these additional services have been required and new application areas investigated, this set of architectures has expanded.

Note that the monitor and host in a treaty verification system are adversaries but are bound to each other and they both operate within the same system. The fact that they are adversaries is another way of saying that it is in each of their interests to cheat. The monitor and host are similar to the customer and merchant who are using electronic transfer. The customer stands to gain if the merchant does not notice the phoney credit card; the merchant stands to gain if the customer does not notice additional charges. However, in the game that the monitor and host are playing the stakes are qualitatively higher. The monitor and host are also similar to the two parties of the prisoner's dilemma, except that cheating might never be evident to either party.

There are three general application areas of remote monitoring architectures. The architecture can monitor an object, a process, or an activity.[2] An example of an object is a unit of weapons-grade material or an actual nuclear weapon. An object could also be a facility such as a storage site. An example of a process is the mixing, under treaty, of weapons-grade uranium with non-weapons-grade uranium to form non-weapons-grade uranium. An example of an activity is seismic activity, particularly seismic activity that would reveal the explosion of nuclear devices. In all of the examples the stakes are high and the adversary, if there is one, is intensely interested in cheating.

Introduction

This paper presents a taxonomy, in the form of an abstract model, of remote monitoring architectures. We will define each of these terms.

A taxonomy shows the relationship between any two individuals in the set covered by the taxonomy.

A model is a representation. For example, the model of a building represents some aspect of the building; but the model is not the building itself, it only represents the building. Since such a model represents a particular building, it could be referred to as a concrete model. On the other hand, an abstract model, for buildings, could consist of generic walls, floors, and ceilings from which a concrete model could be constructed.

Remote monitoring is the observation, at a distance, of an activity that cannot or may not be observed close-up, because it occurs on foreign soil, for example, or because it involves hazardous materials.

An architecture, for our purposes, is a design that organizes computers, sensors, and communication lines.

This paper thus presents a way to determine the relationship between any two designs for the observation, via computers and sensors, of activity on foreign soil or of hazardous material.

There are three components to our model. The first component is the set of parts—sensor, server, and user. The second is the kinds of users, the levels of data sensitivity, and the categories of secure services. The third component is the type of the flow of data between the parts. We use the above components to construct six basic partitions, named Push, Pull, and so on. In each of these partitions there are a number of sub-partitions.

The rest of this paper is organized as follows. In the section Components, we present the components of our model. In the section Partitions, we present the six basic partitions, and then we show some of the sub-partitions. In the section Sample Architectures, we present several architectures, most of them quite general, and show where they fit in our taxonomy.

Components

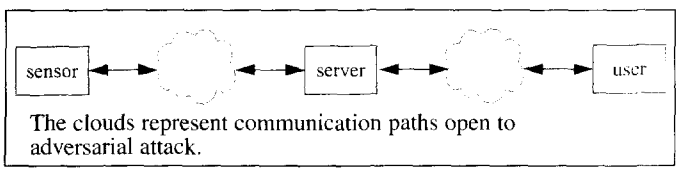
In this section we present the three components of our model. The first component is the set of parts: a sensor, an optional server, and a user, with communication lines connecting sensor and server and connecting server and user. (If the server is not present, then the communication line connects the sensor and user directly.) The second component consists of (a) four kinds of users, (b) two levels of what we call data sensitivity, and (c) seven categories of secure services, such as authentication, confidentiality, proof-of-origin, and so on. The third component is the two types of data flow between the parts: the data can be either pushed or pulled.

Each of these three components is discussed below.

Parts: Sensor, Server, User

We have built our model on an abstract model of the remote monitoring architectures known colloquially as the Sjulin-Moore Model.[3] The Sjulin-Moore Model consists of three general parts: a sensor, a server, and a user, with communication lines connecting sensor-server and server-user, as shown pictorially in Figure 1.

Figure 1: Sjulin-Moore Model



The sensor is assumed to be on the host's soil and generates data of interest to the user. If the host is not the user, then the host is assumed to be an adversary of the user. The sensor, server, and user are themselves assumed to be protected from adversarial attack. If the sensor is a seismometer, then it is presumed to be located in a subsurface hole and thus able to report attacks on itself; other sensors may need tamper-indicating enclosures to provide protection. Meanwhile, the communication lines are assumed not to be protected from adversarial attack. Removing the cloud(s) in the figure above denotes protection of the communication line, as will be shown in various figures below. The server is not required to be present. Nonrepudiation is probably of great interest. And there may be many sensors and/or servers and/or users but the model does not represent them.

For ease of discussion, the information flowing toward the user—from left to right in Figure 1—is referred to as sensor data; the information flowing toward the sensor-from right to left in Figure 1—is referred to as commands.

The Sjulin-Moore Model enables us to grasp the set of remote monitoring architectures but, as with any abstraction, it does so at the cost of simplicity. The model ignores at least the following:

- multiple sensors with different generative rates, resolution, power consumption, and command capabilities, aggregated in different ways, operating in different locations under different jurisdictions;
- multiple servers with different functionality—most likely distributed—with different storage capabilities, characteristics, and inter-server communication paths;
- different users and types of users with different combinations of demands, capabilities, and constraints; and
- different communication paths between all parts of the system (e.g., direct sensor-to-user communication in a system with a server).

Users, Data Sensitivity, and Secure Services

We augmented the Sjulin-Moore Model by defining (a) four kinds of users, (b) two levels of data sensitivity, and (c) seven categories of secure services. Each of these is presented in this section.

Not every kind, level, or category is reasonable with every other kind, level, or category. As a result, of the 56 possible combinations, we consider only 10, all of which are enumerated in this paper.

Users

The users of remote monitoring architectures divide into four groups:

- Host—the owner of the soil on which the sensor is placed;
- Interested party—an organization that has no power over the host and is not in a treaty agreement with the host but for whom the host is willing to provide access to certain information, perhaps to show that the host is a good world citizen;
- Monitoring organization—an organization that is officially recognized internationally and thus has at least the power of world opinion;
- Treaty partner—a party that has entered into a treaty with the host.

Note that in the case of the treaty partner the adversary is not an unidentified rogue whose presence may not even be detected. Rather, the adversary is a legitimate user of the system. Recent history has shown that some parties can consider a monitoring organization to be just as adversarial as a treaty partner.

Data Sensitivity

We presume that all information in the system is assigned one of two sensitivity levels to which we will give the names classified and unclassified. The names we have chosen imply nothing about the characteristics, such as the format, of the associated information. Classified information is always protected at least as well as unclassified. And unclassified information can be shared with at least as many people as classified.

In the current application areas for remote monitoring architectures, classified information is highly protected and never shared with individuals that have not received a clearance. We presume that no foreign nationals would have clearances and thus classified information would never be shared with them. Generally we presume that it is acceptable to share unclassified information with a broader population base than classified information, but restrictions would almost always still apply.

Secure Services

The seven secure services that we consider are integrity, authenticity, freedom-from-inference, confidentiality, and three non-repudiation services—proof-of-origin, proof-of-submission, and proof-of-receipt.[4]

Integrity is protection against unauthorized data modification—the assurance that the data received is the same as the data sent. Authenticity is protection against impersonation—the assurance that the data actually came from the sender. Note that authenticity implies integrity. Note also that proof-of-origin implies authenticity.

Freedom-from-inference is the assurance that no one other than the receiver can make inferences based on the data that is sent to the receiver. For example, if data is sent only when a receiver makes requests, then the presence or absence of data being sent to the receiver may allow someone to make inferences about the receiver's interests. Note that the data itself is not the concern here since it may be unclassified and available to all. One way to provide freedom-from-inference is to send data that is not requested. Another way is to provide confidentiality, which is the protection against eavesdropping, the assurance that no one other than the receiver has been able to see the data in its cleartext form, though others may have seen it in its ciphertext form. For simplicity's sake we will define confidentiality to include freedom-from-inference.

Proof-of-receipt implies proof-of-submission. But there are situations in which both may be required. For example, suppose that the communication line between the sensor and the user is highly variable in its delivery time (we are assuming for the moment a system that has no server). Assume also that the host wants to be able to prove that the user has received the data. In this situation both services may be required, proof-of-submission to be able to prove that the data is on its way, and proof-of-receipt to be able to prove that the data actually arrived. Or, to protect against an unreliable server, the host could require that the server provide proof-of-receipt on data sent to the server, and the user could require proof-of-submission on data sent from the server. Note that in this last scheme the host does not have proof-of-receipt from the user, nor does the user have proof-of-submission from the host. This enables both parties to protect against an unreliable server at the same time not providing their adversary unnecessary power.

We presume that authenticity is required on all communication lines because none of the parties may be able to corroborate the information flow via another source.[5] Also, the information may lose all value if it is not authenticated. For example, seismometer data is essentially worthless without knowing the

Table 1: Combinations of Data Sensitivity & Secure Services

	data classified?	confidentiality?	proof-of-		
			-origin?	-submission?	-receipt?
1	no	no	no	no	no
2		yes			
3	yes[a]				
4	no		yes		
5			no	yes	
6				no	yes
7				yes	
8			yes		no
9				no	yes
10				yes	

a. This is the only case in which the user can only be the host. In all other cases the user can be any one of the four kinds—host, interested party, monitoring organization, or treaty partner.

location of the seismometer. We also presume that freedom-from-inference is required on all communication lines. As a result of these two presumptions, the seven secure services reduce to four: confidentiality and the three non-repudiation services.

Combinations

Combining each kind, level, and category we can generate 4*2*7 = 56 combinations. Many of those combinations are superfluous. There are constraints on the secure services, noted above, that reduce their number from seven to four. We presume that classified information would always be given confidentiality. Similarly, if the data is classified, then the user is always the host, simply because the only time that the host would allow classified information to be transmitted to the user is when the user is in fact the host; when the data is unclassified, the kind of user does not differentiate combinations. However, when we present sub-partitions, we will show how the nature of the systems in those sub-partitions implies the nature of the users. As a result of these constraints, the 56 possible combinations reduces to the 10 shown in Table 1.

Types of Data Flow

We assume two types of data flow in the model—push and pull-based on the absence or presence of commands, respectively. In a push communication the data is sent without being in response to a command. In a pull communication the data is sent in response to a command.

Partitions

In this section we first present the basic partitions, and then we show the sub-partitions, using the data sensitivity and secure services combinations shown in Table 1.

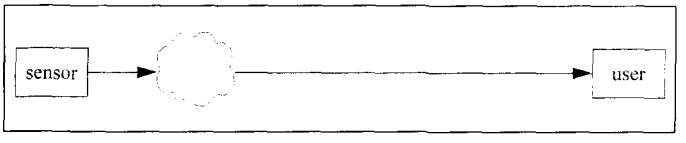
Basic Partitions

The presence/absence of the server and the directionality of the remaining communication lines (push or pull) results in six partitions: Push, Pull, Push-Push, Push-Pull, Pull-Push, and Pull-Pull. A diagram for each partition is shown in a figure below. There are a number of systems in each partition.

The diagram for the systems in the Push partition is shown in Figure 2.

There is no server in these systems and the user is unable to issue commands. Since there is no command flow to the sensor, these systems can provide a higher level of security than any of the Pull systems can. It is possible for different users to be connected to different sensors, but every user that is connected to a given sensor is sent all of the information in real-time[6] that is generated by that sensor.

Figure 2: The Push Partition



(If proof-of-receipt were required by the sensor, then the system would have to provide a flow from the user. However, since this flow would not include commands, then imposing the requirement for proof-of-receipt would not place a system in the Push partition into a system in a pull partition. That is, it is the presence of commands that put systems into a Pull partition.)

The diagram for the systems in the Pull partition is shown in Figure 3.

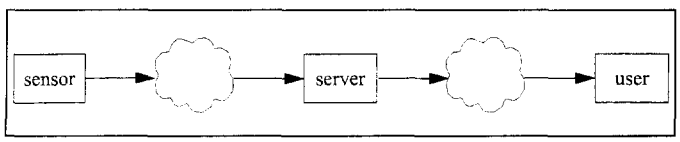
Figure 3: The Pull Partition

Like the systems in the Push partition, the systems in the Pull partition have no server. However, the user is able to issue commands. The diagram does not specify the extent of the control that the user has over the sensor—it may be minuscule. It is possible with systems in this partition that the user could ask for changes in the sensors based on the sensor

data itself. For example, if the data from a bank of sensors suggested that a seismic event were occurring, the user could ask for an increase in sensing frequency for the sensors in the area of interest. Additionally, the user could direct cameras toward a door whose alarm has just been triggered. Again, like the systems in the Push partition, it is possible for different users to be connected to different sensors, but it is assumed that every user connected to a given sensor is sent all of the information that is generated by that sensor in real-time.[7]

The diagram for the systems in the Push-Push partition is shown in Figure 4.

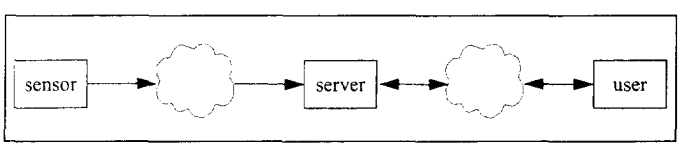
Figure 4: The Push-Push Partition



The systems in this partition have a server but no commands can be issued. The presence of the server implies that there is storage available—the sensor data is no longer required to flow to the user in real-time as it was in the Push and Pull partitions. The server may provide the raw data to the user; but on the other hand it may condense it, change its classification, or massage it in some way. There may be multiple servers and they may be connected serially, making it possible for the same user to receive the same sensor data in raw, condensed, differently-classified, and massaged form. But note that the user cannot direct the server and the server cannot direct the sensor.

The diagram for the systems in the Push-Pull partition is shown in Figure 5.

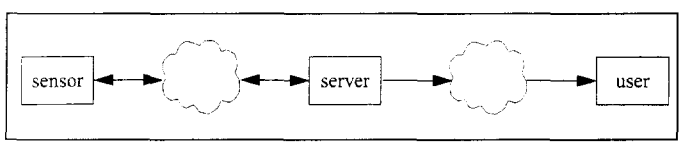
Figure 5: The Push-Pull Partition[a]



a. The IAEA currently requires sensors to have the "store and forward" capabilities shown in this model.

The systems in this partition have a server, as in the previous partition, but the user can issue commands, at least to the server. This enables the user to direct the distribution of raw data and/or direct the massaging of data, at least to some extent. But note that since the server cannot issue commands, neither the server nor the user can direct any of the activities of the sensor.

Figure 6: The Pull-Push Partition

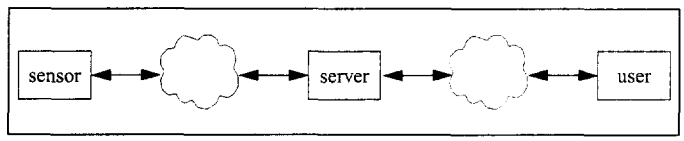


The diagram for the systems in the Pull-Push partition is shown in Figure 6.

The systems in this partition allow the server to direct the activities of the sensor—the user has no opportunity to direct either the server or the sensor. Systems in this partition are presumed to have built sufficient intelligence into the server that commands from the user are not needed. It may be that the user is not trusted; or it may be that this approach is adopted because it reduces the traffic from the user to an acceptable level.

The diagram for the systems in the last partition, the Pull-Pull partition, is shown in Figure 7.

Figure 7: The Pull-Pull Partition



The systems in this partition allow the server to direct the activities of the sensor and also allow the user to direct the activities of the server, at least potentially. It may be that the server can pass user commands on through to the sensor. But on the other hand the server could filter such commands or disallow them entirely, letting only its own commands be issued to the sensor.

Sub-Partitions

We can further partition the Push/Pull partitions presented above by applying the combinations of data sensitivity and secure services, shown in Table 1, to each of the communication lines in each partition. Since there are 10 possible combinations, the number of representative systems in each partition depends on the number of available, unidirectional communication lines. There is only one unidirectional communication line in the Push partition, for example, but in the Pull partition there are two—one for data from the sensor to the user, and one for commands from the user to the sensor. Table 2 shows the number of representative systems in each partition.

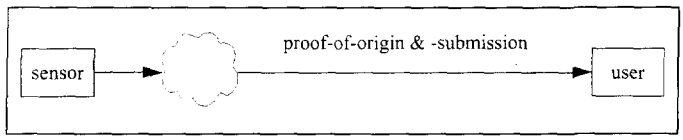
Table 2: The Partition Sizes

Partition	Communication Lines	Partition Size
Push	1	$10^1 = 10$
Pull	2	$10^2 = 100$
Push-Push		
Push-Pull	3	$10^3 = 1{,}000$
Pull-Push		
Pull-Pull	4	$10^4 = 10{,}000$

We show examples from the Push, Push-Push, and Pull-Pull partitions below.

As an example of one of the 10 systems in the Push partition, consider Figure 8.

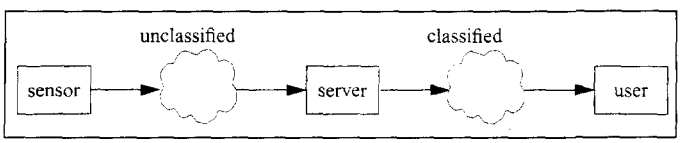
Figure 8: A Push System



The communication line to the user provides proof-of-origin to the user and proof-of-submission to the sensor. Since proof-of-origin is provided we can conclude that the user is probably a monitoring organization or a treaty partner but not the host or an interested party: the host would not need proof-of-origin and would not allow it for an interested party. Since the sensor is provided proof-of-submission we know that the host is interested in being able to prove to a third party that the data was in fact sent. This, in itself, does not narrow the field of possible users. However, note that the sensor is not provided with proof-of-receipt. The reason for the absence of this service suggests politics: with proof-of-submission the sensor can be free of blame without simultaneously being obliged to show negligence on the part of the user-noise on the communication line, for example, can always be called on to account for missing data. We conclude that the user is a treaty partner.

As an example of one of the 100 systems in the Push partition, consider Figure 9.

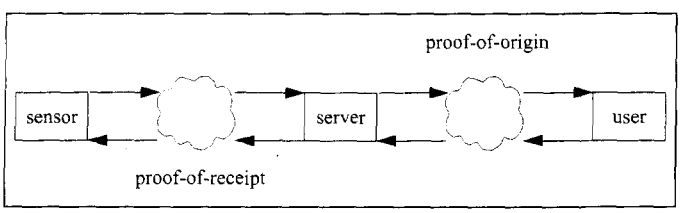
Figure 9: A Push-Push System



The user is the host since the communication line delivers classified to the user. The data from the sensors is unclassified, so the server must be condensing or correlating or massaging the data in some way that it becomes classified.

As an example of one of the 10,000 systems in the Pull-Pull partition, consider Figure 10.

Figure 10: A Pull-Pull System



The user is provided proof-of-origin from the server but not from the sensor. We can conclude from this that the user trusts the sensor but not the server. The server is not provided non-repudiation in its communication to the user. We can conclude from this that the server is not held accountable for not sending data. Meanwhile, the server is provided proof-of-receipt for its commands to the sensor. We can conclude from this that the server does not trust the sensor. The sensor and server do not belong to the same party, neither do the server and user.

Sample Architectures

In this section we present high-level, logical views of several remote monitoring architectures, namely:

- Self-Aware Weapon / Information Infrastructure (SAW/II),
- Integrated Intrusion Detection and Access Control Annunciator (IDACA),
- Modular Monitoring System (MMS),[8]
- International Monitoring System for the Comprehensive Test Ban Treaty (CTBT IMS), and
- an architecture for monitoring fluid mix.

The general nature of the designs implies that most of them fall into the most general partition, Pull-Pull. Table 3 categorizes the architectures based on the partitions presented here.

Table 3: Summary of Sample Architectures

Architecture	Push/Pull	Data Sensitivity	User
SAW/II	Push-Pull	classified	(any but treaty partner; *the classified data would* be declassified if the user were a monitoring organization)
IDACA	Pull-Pull	unclassified	Host
MMS	Push-Pull or Pull-Pull, depending on the implementation	unclassified, available to unclassified and classified users	(any)
CTBT IMS	Pull-Pull	unclassified	Treaty partner
Monitoring fluid mix	Push	unclassified	Treaty partner

The architecture for SAW/II is shown in three figures—Figure 11, Figure 12, and Figure 13. Each subsequent figure expands on the previous one.

Figure 11: SAW/II System Architecture

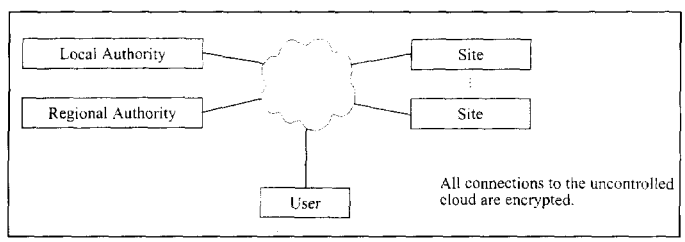
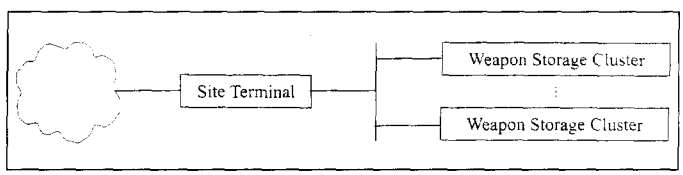
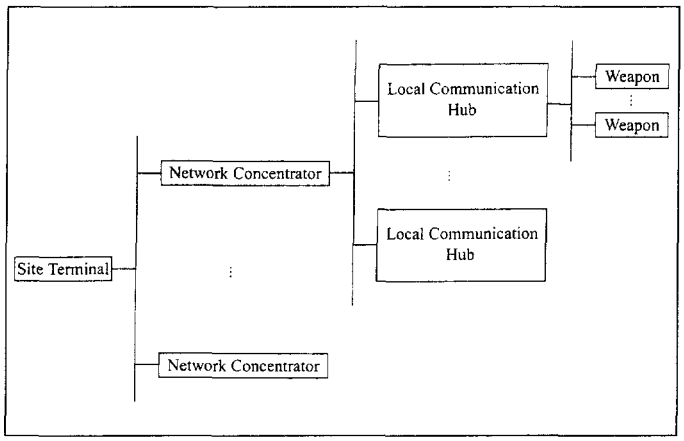


Figure 12: SAW/II Site Architecture



SAW/II is intended to be used with nuclear weapons. It is assumed that the weapons are geographically dispersed and that the sensing devices on the weapons themselves are expected to operate for long periods of time on battery power alone. The architecture presumes that the sensing devices push the data to the servers; this has a security aspect to it, besides

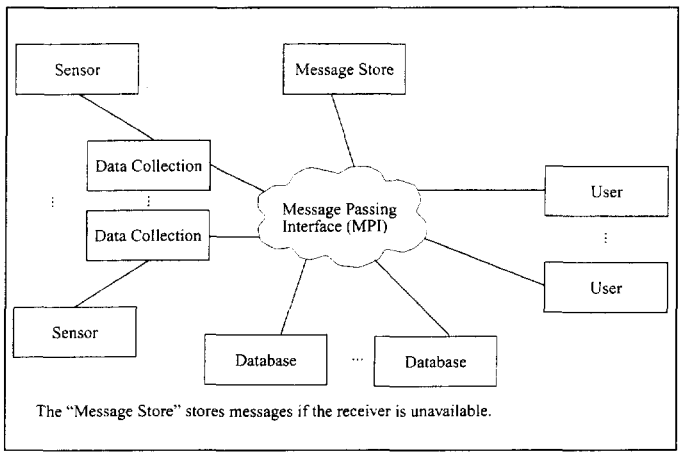
Figure 13: SAW/II System Architecture



the practicality of reducing the drain on precious power—and that users can pull information from the servers at each site. Hence this architecture is in the Push-Pull partition. The large number of layers in the architecture reflects the expected geographical distribution, the need to be able to process commands away from the sensors, and the expected highly diverse user population.

The MMS architecture is shown in Figure 14.

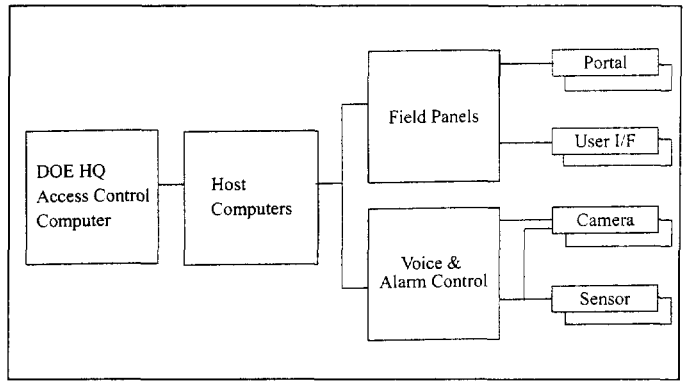
Figure 14: MMS System Architecture (logical view)



MMS is intended to monitor materials. The data from the sensors funnels to data collection controllers. Not shown in the figure are the storage controller unit and the site controller unit, which act as servers. MMS is a Push-Pull or a Pull-Pull system, depending on the implementation. One alternate design splits the communication line, sending classified information on one network and unclassified information on another. In this alternate design, commands from the classified network are not allowed to proceed back to the sensor, making this a Push-Pull system. Regardless of these alternatives, we would expect a wide variation in the filtering of commands from the user to the sensors.

The IDACA architecture is shown in Figure 15.

Figure 15: IDACA Architecture



IDACA was designed for monitoring sites within the U.S. Department of Energy. The variety of sensing devices indicates the variety of activities that this architecture is intended to monitor. There would be one set of host computers at each site. These machines would be responsible for alerting security personnel of problems. The HQ computer would provide information between sites. This architecture has a server in the field panels and voice and alarm control, yet users are also assumed to be able to direct the various sensors, so this architecture is in the Pull-Pull partition.

The CTBT IMS architecture is shown in Figure 16, Figure 17, and Figure 18.

Figure 16: Logical Structure of CTBT IMS

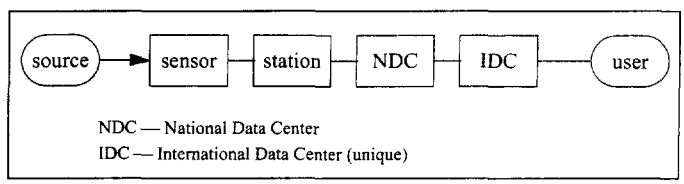


Figure 17: CTBT IMS Architecture

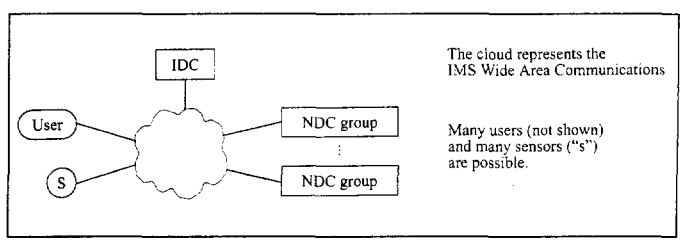
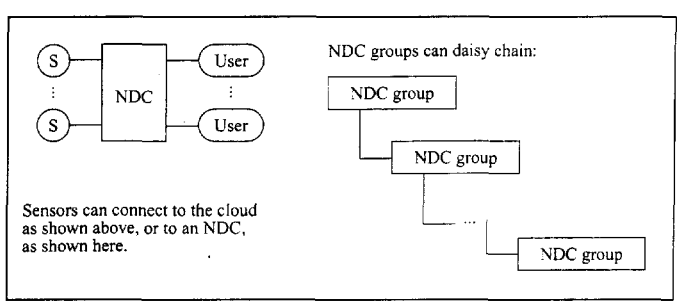


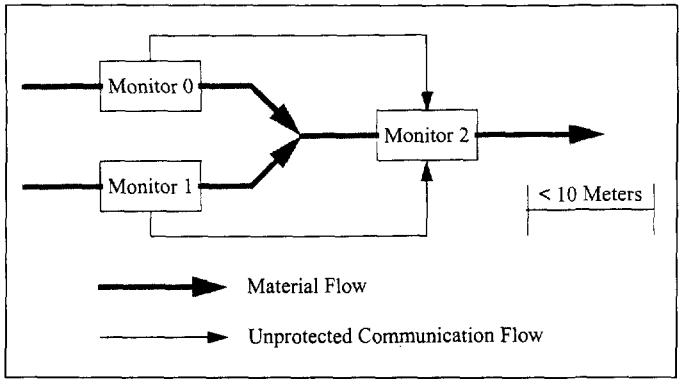
Figure 18: National Data Center (NDC) group



The logical structure of CTBT IMS is similar to StraightLine, upon which MMS is based, except that CTBT IMS has a single hub, the IDC. This single point is intended to control the flow of all data and commands. As we would expect, the architecture does not rule out the possibilities for users to receive data from sensors in their own countries without going through the IDC. This architecture is in the Pull-Pull partition.

An architecture for monitoring material fluid mix is shown in Figure 19.

Figure 19: Logical Structure of CTBT IMS



The scale indicates correctly that this architecture is designed to be used within a single building, on the adversary's soil, within a secured compound also controlled by the adversary. The user is an inspector that is provided periodic on-site access to the output of Monitor 2 and monitored inspection of the other monitors to check for component failures (i.e., attempts by the adversary to subvert the tamper-indicating enclosures that surround the monitors). Since the user can issue no commands and since there is no server, this architecture is in the Push partition.

Acknowledgments

We appreciate the review of previous versions of this paper by Brad Mickelson, Curt Nilsen, Don Glidewell, John Matter, Keith Tolk, and Reynold Tamashiro, all of Sandia National Laboratories.

Notes

1. Non-repudiation, for our purposes, is the capability of being able to prove to the satisfaction of a mutually-agreed-upon third party, one or more of the following about the transmission of a given unit of data: the identity of the person from whom the data originated, known as "proof-of-origin;" that the data was in fact sent, known as "proof-of-submission" (note that this says nothing about whether or not the data ever arrived, only that it was submitted); that the data was in fact received, known as "proof-of-receipt." Assuming that proof-of-submission never arrives before the data itself, the receiver of the data is interested only in the first capability, whereas the sender of the data is interested in both of the other two capabilities.
2. As an aside, in the area of international safeguards there are three general applications: storage, transportation, and process.
3. This model is named after its developers, Mike Sjulin (pronounced shah-LIN, rhyming with pa-DIN) and Judy Moore of Sandia National Labs. It is an abstraction of the "Notional Remote Monitoring System."
4. See note 1 for a definition of non-repudiation services.
5. The International Atomic Energy Agency currently requires authentication at the data source (i.e., of the sensor data) and that all data transmitted from member nations to the IAEA be encrypted.
6. Some applications require built-in delays.
7. See previous note.
8. MMS is a follow-on to both the Modular Integrated Monitoring System and Straight-Line, neither of which is shown in this document.

References

R. L. Craft, "A Somewhat Definitive Guide to the Potential Future Needs of Information Surety at Sandia National Labs." November 1996.

D. R. Hofstadter, "Metamagical Themas: Questing for the Essence of Mind and Pattern." Basic Books, New York. 1985.

G. J. Simmons, "How to Insure that Data Acquired to Verify Treaty Compliance Are Trustworthy." Proceedings of the IEEE, vol. 76, no. 5. May 1988. (Reprinted as Chapter 13 of "Contemporary Cryptology," edited by G. J. Simmons, IEEE Press, 1992.)

G. J. Simmons, R. E. D. Stewart, P. A. Stokes, "Digital data authenticator." Patent Application SD2654, S42640, June 30, 1972.

Peter Wayner, "Digital Cash: Commerce on the Net." Academic Press Limited, London. 1997. ISBN 0-12-788772-5.

Private communication with Bradley J. Wood of Sandia National Laboratories.

The Role of Expert Judgment in Safeguards

William D. Stanbro and Kory Budlong-Sylvester
Safeguards Systems Group
Los Alamos National Laboratory
Los Alamos, New Mexico, U.S.A.

Abstract
Use of expert judgment is a common component in designing and evaluating safeguards systems. This is a trait that safeguards shares with many different fields. There has been a trend to formalize expert judgment procedures in a number of different areas. These procedures are believed to result in greater reliability and acceptance of decisions made in this manner. There is a strong argument for implementing such formal procedures in safeguards, but this should be done in a graded manner after carefully considering factors such as cost and complexity.

Introduction
Like most engineering projects, establishing and supporting a safeguards system at a nuclear facility is based on a series of tradeoffs between efficacy and cost. Ideally such tradeoffs would be based on detailed quantitative analyses of the ability of system elements to detect or deter theft or diversion of nuclear material with detailed cost estimates. In practice, such analyses are difficult or impossible for some elements of a safeguard system. In this type of situation, processes based on expert judgment are commonly used in many fields (forensics,[1] medicine,[2] environmental management,[3] and nuclear safety analysis[4]). The form that the expert judgment takes can be classed as either informal or formal. Informal expert judgment tends to not follow set procedures, may be poorly documented, and is not very clear. Formal expert judgment, often called expert elicitation, uses structured procedures to clarify the reasoning of the expert and stresses the need for good documentation.[5]

This paper will examine the use of expert judgment that has occurred in other fields. This will be followed by a discussion of how this experience may be used to improve the use of expert opinion in safeguards.

Use of Expert Judgment Outside of Safeguards
Forensics
The legal system has long used expert judgment to illuminate technical areas beyond the realm of the ordinary layman. Traditionally in the United States, this type of testimony has been fairly freewheeling; it is often left to judges and juries to choose between opposing views. More structured approaches may be found in some other countries,[6] and the situation is changing even in the United States. In a 1993 U.S. Supreme Court decision (*Daubert v. Merrell Dow Pharmaceutical, Inc.*), judges are required to prescreen scientific expert opinion to see that it is formed in a *scientifically valid manner.*[1] This was extended to other expert judgment in *Khumo Tire vs. Carmichael.*[7] In *Daubert*, the Court established several principles for determining validity:

- "Can (and has) the method in which the expert's conclusions are reached be tested or—in the terminology of scientists—falsified?
- Has the theory been peer reviewed and published?
- What is the known or potential rate of error of the scientific technique, and are there standards controlling the technique's operation?
- Is the theory or technique generally accepted in the relevant scientific community?"[7]

While in Khumo the court held that this list varied from discipline to discipline and some flexibility was allowed,[7] it is clear that the U.S. legal community is being called to a more structured use of expert opinion.

Medicine
The medical community is currently involved in a lively debate on the role of traditional and informal forms of expert judgment.[2,8-12] One part of this community has advanced the opinion that decisions on patient care should be made on the basis of randomized controlled trials in preference to qualitative judgments based largely on the experience of the physician.[13] A suggested hierarchy of confidence is shown in Table I. This table places expert judgment as the least reliable source of evidence for making decisions on patient care. Opinions of this new approach range from the use of well-run clinical trials and doubts about the reliability of expert opinion to problems with clinical trials and the unavailability of appropriate studies. From the viewpoint of an outsider these debates suggest that there are circumstances in which either approach is correct.

Environmental Management
Professionals in environmental management and control are

Table I. United States Preventive Services Task Force Ratings for Quality of Evidence

Rating	Description
I	Evidence from at least properly randomized controlled trial.
II-1	Evidence obtained from well-designed controlled trials without randomization.
II-2	Evidence obtained from well-designed cohort or case-control analytic studies, preferably from more than one center or research group.
II-3	Evidence obtained from multiple time series with or without the intervention. Dramatic results in uncontrolled experiments (such as the results of the introduction of penicillin treatment in the 1940s) could also be regarded as this type of evidence.
III	Opinions of respected authorities, based on clinical experience; descriptive studies and case reports; or reports of expert committees.

often presented situations in which there is no clear-cut solution known. It is common for these cases to be tackled through the use of expert judgment. Increasingly, however, more formal forms of expert opinion are being used because of the higher utility of these types of decisions.[3,14,15]

Nuclear Safety Analysis

The area of nuclear safety analysis has the most expertise in using formal expert judgment.[16-21] Much of this has been sparked by the need to obtain parameters for risk assessments using the technique of probabilistic risk assessment.[22] Initially, these assessments used informal processes to elicit information. However, these were strongly criticized for their inherent biases, lack of documentation, and their inability to address uncertainty. This led to the implementation of more formal procedures that significantly enhanced the credibility of future studies.[16] One such study is used as the basis of the example in the next section.

How Expert Elicitation Might Be Used in Safeguards

The process described here is based on the expert elicitation process used in the preparation of the reactor safety study, NUREG-1150.[23] The methodology used in this study has been placed in the context of a safeguards regulatory body that requires detection probabilities for various safeguards measures.

The expert elicitation process is divided into seven steps.[16]

1) Identify and select issues.
2) Identify and select experts.
3) Discuss and refine the issues.
4) Train for elicitation.
5) Elicitation.
6) Analyze, aggregate, and resolve disagreements.
7) Document and communicate.

A necessary precondition for this sort of analysis would be the establishment of a group within the SRB with the expertise in both safeguards and expert elicitation to conduct such exercises. Another addition might be a committee to review the results and provide a level of quality assurance.

Identification and selection of issues

In general, it is neither possible nor desirable to assemble expert panels to determine all probabilities. Wherever possible, engineering analyses and the results of previous studies should be used. Further, some questions may be so straightforward that judgments can be made on an informal basis with little impact on the acceptability of the product. Further prioritization may come from judgments about the relative importance of particular measures in a given system. This sort of selection process should use formal guidelines that are uniformly applied.

Identification and selection of experts

A well-rounded panel of experts is obviously the key to any expert elicitation process. It may be desirable for the SRB group responsible for assembling the panel to seek suggestions from outside committees. A good panel should be composed of both specialists in the area being addressed and generalists who bring a broader perspective.[1]

Discussion and refinement of the issues

In this step, the expert panel and the SRB elicitation group should meet. The purpose of the meeting is to describe the question under discussion and to explain what input is desired from the panel. The panel has the chance to mutually discuss the issue, and if possible to agree on a how to divide the problem parts. Such an agreement will help ease the burden of developing the final recommendations, but it is not necessary.

Training for elicitation

The first meeting between the panel and SRB elicitation group is also an opportunity to train the expert panel on the process of elicitation and the form that their input should take. This step appears to be particularly necessary in cases involving estimation of probabilities.[4,16]

Elicitation

The actual elicitation can take many different forms.[4] The method used in the NUREG-1150 case 16 is described here. It consisted of individual, in-person interviews in which a series of questions were asked. Generally, the questions moved from easy to hard. At each stage the expert was asked to explain his or her reasoning. During the questioning, the SRB group examined the results for consistency and documented the entire process.

Analysis, aggregation, and resolution of disagreements

At this stage the results of the elicitation process for each expert are put into a consistent form, and the results from all of the experts are aggregated. In some instances a meeting of all experts may be convened to further understand the basis for areas of both disagreement and agreement.

Documentation and communication

A clear advantage of a formal elicitation process is its transparency. A complete documentation of the process is available for review along with the results. Experience has shown that this results in increased acceptance of the product.[16]

Options for Expert Elicitation

It should be emphasized strongly that a large number of options have been developed for the elicitation step and the analysis, aggregation, and resolution of disagreements step.[4] The choice of which to pick can be made on the basis of such factors as the time available to obtain the needed results, the ease of assembling the experts, the group dynamics of the expert panel, and, most importantly, the cost.

Some of the major options concern the level of interaction of the panel members. For example in the Delphi process, panel members never meet. The elicitation often takes place remotely by telephone or mail. Panel members then are sent digested summaries of panel members' positions to which they are asked to respond. Several iterations of this type of process are often employed in an attempt to achieve conscensus.[4]

Other techniques use individual interviews, as in the case described above, or meetings of the entire panel for direct discussion of the issues. Each approach has is own advantages and disadvantages and can be tailored for aparticular situation.[4]

The analysis of the results of elicitation is also a vital part of the use of formal expert judgment. While sometimes done in an ad hoc manner, a more structured approach than the one described in the NUREG-1150 example can lead to a much better understanding of the results, including the ability to detect biases and estimate uncertainties. These approaches are based on the use of statistical techniques such as simulation modeling and Bayesian statistics.[4]

Conclusions

Decision makers will continue to be faced with making choices in areas that are not amenable to rigorous scientific and engineering analysis. Various parts of safeguards systems are likely to fall into this category. In these situations, it will be appropriate that the decision makers turn to experts to help them solve their problems. As has been shown in this paper, safeguards is not unique in this respect. Also, as in other fields, safeguards managers can expect to be confronted with the need to explain and justify their decisions. In other words, there will be increased requirements for the decision making process to be well-documented. In these cases the use of formal expert elicitation procedures can provide increased confidence that decisions are being made on the best available evidence and that the decision process can be demonstrated to be a logical outcome of this evidence. This has been shown to not only improve the quality of the expert judgment process but also to increase its acceptability to stakeholders.

A challenge in the use of formal expert judgment, however, is to use an appropriate level of formality for each individual decision. The level of effort employed in making a decision should be commensurate with the importance and complexity of the decision. Safeguards professionals are well aware of the use of "graded" approaches. The same should apply to the use of formal expert judgment. It only should be employed in some situations, and then only to the degree warranted by the particular situation.

William D. Stanbro is employed by Los Alamos National Laboratory, where he is a technical staff member in the Safeguards Systems Group of the Nonproliferation and International Security Division. He received a bachelor's degree and a doctorate in physical chemistry from George Washington University and a master's degree in computer science from Johns Hopkins University. His background includes work in environmental science, medical research, nuclear safeguards and technical aspects of national security issues.

Kory Budlong-Sylvester is employed by Los Alamos National Laboratory, where he is a technical staff member in the Safeguards Systems Group of the Nonproliferation and International Security Division. He received his doctorate in nuclear engineering from MIT. His primary areas of expertise are radioactive waste management and nuclear fuel cycle engineering.

References

1. Rodricks, J. V. and S. H. Rieth. 1998. Toxicological Risk Assessment in the Courtroom: Are Available Methodologies Suitable for Evaluating Toxic Tort and Product Liability Claims? *Regulatory Toxicology and Pharmacology* 27:21-31.
2. Vandenbroucke, J. P. 1998. Observational Research and Evidence-Based Medicine: What Should We Teach Young Physicians? *J. Clin. Epidemiol.* 51(No. 6):467-472.
3. Stiber, N. A., M. Pantazidou, and M. J. Small. 1999. Expert System Methodology for Evaluating Reductive Dechlorination at TCE Sites. *Environ. Sci. Technol.* 33:3012-3020.
4. Meyer, M. A. and J. M. Booker. January 1990. Eliciting and Analyzing Expert Judgment. NUREG/CR-5424.
5. Otway, H. and D. von Winterfeldt. 1992. Expert Judgment in Risk Analysis and Management: Process, Context and Pitfalls. *Risk Analysis* 12:83-93.
6. Leinzinger, E. P. 1999. Penal and Civil Liability of the Medical Expert Witness in the Austrian Legal System,. *Forensic Science International* 103(No. S1):S21-S23.
7. Case, D. T. and J. B. Ritter. February 21, 2000. Disconnects Between Science and the Law. *Chemical and Engineering News,* 49-60.
8. Costa, A. and S. M. Hubbard. 1997. Evidence Based Medicine, a New Challenge. *European Journal of Cancer* 33(No. 7):987-988.
9. Funai, E. F. 1997. Obstetrics & Gynecology in 1996: Marking the Progress Toward Evidence-Based Medicine by Classifying Studies Base on Methodology. *Obstetrics & Gynecology* 90:1020-1022.
10. Benitez-Bribiesca, L. 1999. Evidence-Based Medicine: A New Paradigm? *Archives of Medical Research* 30:77-79.

11. Lopez-Jimenez, F. and G. A. Lamas. 1999. Evidence-Based Medicine. *Archives of Medical Research* 30:80-81.
12. Earle, C. C. and J. C. Weeks. 1999. Evidence-Based Medicine: A Cup Half Full or Half Empty? *Am. J. Med.* 106:263-264.
13. Evidence-Based Medicine Working Group. 1992. Evidence-Based Medicine, A New Approach to Teaching the Practice of Medicine. *JAMA* 268(No. 17):2420-2525.
14. Morgan, M. G. and D. W. Keith. 1995. Climate Change: Subjective Judgments by Climate Experts. *Environ. Sci. Technol.* 29(No. 10):A468-476.
15. Bishop, G. D., M. R. Church, J. D. Aber, R. P. Neilson, S. V. Ollinger, and C. Daly. 1998. A Comparison of Mapped Estimates of Long Term Runoff in the Northeast United States. *Journal of Hydrology* 206 (No. 3-4):176-190.
16. Keeney, R. L. and D. von Winterfeldt. 1991. Eliciting Probabilities from Experts in Complex Technical Problems. IEEE Transactions on Engineering Management 38(No. 3):176-190.
17. Helton, J. C., R. J. Breeding, and S. C. Hora. 1992. Probability of Containment Failure Mode for Fast Pressure Rise. Reliability Engineering and System Safety 35 (No. 2):91-106.
18. Dewispelare, A. R., L. T. Herren, and R. T. Clemen. 1995. The Use of Probability Elicitation in the High Level Nuclear Waste Regulation Program. *International Journal of Forecasting* 11(No. 1):5-24.
19. Miklas, M. P., J. Norwine, A. R. Dewisplare, L. T. Herren, and R. T. Clemen. 1995. Future Climate at Yucca Mountain, Nevada Proposed High Level Radioactive Waste Repository. Global Environmental Change-Human and Policy Dimensions 5 (No. 3):221-234.
20. Zio, E. and G. E. Apostolokis. 1996. Two Methods for the Structured Assessment of Model Uncertainty by Experts in Performance Assessments of Radioactive Waste Repositories. *Reliability Engineering and System Safety* 54:225-241.
21. Hora, S. C. and D. von Winterfeldt. 1997. Nuclear Waste and Future Societies: A Look into the Deep Future. *Technological Forecasting and Social Change* 56:155-170.
22. Caruso, M. A., M. C. Cheok, M. A. Cunningham, G. M. Holahan, T. L. King, G. W. Parry, A. M. Ramey-Smith, M. P. Rubin, and A. C. Thadani. 1999. An Approach for Using Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis. *Reliability Engineering and System Safety* 63:231-242 (1999).
23. Nuclear Regulatory Commission. 1989. Several Accident Risks: An Assessment of Five U.S. Nuclear Power Plants. Summary Report, NUREG-1150.

Physical Protection Performance Testing: Assessing U.S. NRC Experience

Oleg Bukharin
Princeton University
Princeton, New Jersey, U.S.A.

Abstract
Performance testing is an essential component of an effective, sustainable system of nuclear safeguards and security. This paper provides an overview of physical protection performance testing programs developed by the U.S. Nuclear Regulatory Commission to evaluate security of nuclear power plants and discusses their impact on licensee security programs. The paper then addresses potential difficulties of implementing a performance testing program and discusses why the NRC programs have been generally successful.

Introduction
The United States is working cooperatively with Russia to improve nuclear material protection, control and accounting at tens of sites of the Russian nuclear complex. Rapid upgrades have been completed at more than 20 facilities but their effectiveness remains uncertain. There is also a concern that newly improved security systems might not be sustainable over time without a fully developed safeguards culture and effective regulatory oversight. Nuclear safeguards and security is believed to be inadequate against today's threats at many facilities in some countries as well. The development of nuclear safeguards in the United States can offer valuable lessons that could help addressing these problems.

Nuclear materials and facilities in the United States are probably more secure than anywhere in the world. This, however, has not always been the case. Improvements in safeguards technologies and procedures, a major political and resource commitment, and changes in the mindset of the safeguards community were required to bring nuclear security up to its present level.

Performance testing has been critical to the development and maintenance of the modern safeguards culture and increased safeguards effectiveness. While performance testing is particularly important in the area of physical protection, it has also been employed successfully in material control and other safeguards disciplines.

This report primarily focuses on physical protection performance testing programs developed by the U.S. Nuclear Regulatory Commission to evaluate security of nuclear power plants. Nuclear power plants represent the majority of NRC-licensed high-security facilities.[1] An analysis of power reactor security is also somewhat easier because power plants are less sensitive than category I facilities, where classified national security work is conducted. At the same time, physical protection approaches and much of security hardware and procedures at power reactors are similar to those used to protect special nuclear materials.

Moreover, in some respects the task of securing a nuclear power plant is more demanding. Because of safety and cost considerations, reactor facilities in the United States do not rely on delay mechanisms to the same extent they are relied on at category I facilities. To defend against an external threat, facility's response forces must interdict the adversary before it reaches certain vital equipment (denial strategy). In contrast, some category I facilities utilize the containment strategy, which allows the adversary to reach its targets inside the protected area but requires the security forces to seal off the area to prevent the adversary from escaping until off-site forces arrive to deal with the problem. Finally, reactor security arrangements are in some cases more complex because of the need to take into consideration technical and safety aspects of nuclear power plant operations.

U.S. NRC Regulatory Program: The Need for Performance Testing
The NRC was established in 1974 and its principal regulatory responsibilities include development and maintenance of rules and regulations, licensing, and inspection and enforcement. An emergency response, post-incident investigation, and development and maintenance of a design basis threat (see below) are additional important regulatory functions. The NRC is responsible for the oversight of physical protection programs at 71 nuclear power plants (109 reactors units) and two category I fuel cycle facilities manufacturing 97 percent enriched HEU fuel for the U.S. Navy.[2]

Physical security regulations for NRC-licensed facilities are contained in the U.S. Code of Federal Regulations.[3] Physical protection requirements for nuclear power plants are listed in the part 10 CFR 73.55 and consist of eight paragraphs, from (a) to (h). The paragraph 73.55(a) sets the general performance requirement for a physical protection system to be "designed to

protect against the design basis threat of radiological sabotage." The rules then specify that in order to achieve this objective "the on-site physical protection system and security organization must include, but not necessarily be limited to, the capabilities to meet the specific requirements contained in paragraphs (b) through (h) of this section [73.55]." The paragraphs 73.55 (b)-(h) contain prescriptive requirements regarding a physical security organization, physical barriers (including detection and assessment systems), access control, alarm stations, communication, equipment testing and maintenance, and response.

From the practical standpoint, NRC regulatory activities at a particular facility have traditionally been focused on a physical security plan.[4] The plan, a part of the general operating license, contains a detailed explanation of a facility's physical security programs and elements. The security plan is reviewed by NRC staff during the licensing process to assure that facility's commitments are in line with the requirements contained in the paragraphs 73.55 (b)-(h). It is then assumed that the performance objective of the paragraph 73.55 (a) is also met.

As the facility becomes operational, NRC staff from the corresponding regional office periodically conduct inspections to verify that the licensee meets physical security plan commitments. These inspections are largely administrative in nature and rely on the analysis of facility's records, interviews with security personnel, on-site observations, and inspector judgment.[5]

The described approach could be classified as compliance-based or prescriptive. Generally speaking, under the compliance-based approach, regulatory documents postulate a minimal set of procedures and security hardware that a physical protection system must include. A facility is then subjected to administrative inspections that are carried out against a checklist and are intended to assure that all mandatory physical protection elements are in place and operable.

While the compliance approach is useful to establish baseline capabilities of a nuclear safeguards system, it generally does not provide for an evaluation of its true effectiveness. In other words, a physical security system might comply with prescriptive regulatory requirements but still be unable to fulfill its primary objective—the protection of nuclear materials and facilities. Indeed, NRC's experience indicates, for example, that under the compliance approach "licensee safeguards hardware systems, such as intrusion detection systems and CCTV, would generally be effective against unintentional entry into licensee's protected area, or against attempted covert entry by an unskilled individual. However, at many sites, systems would not be highly effective against a knowledgeable, skilled individual."[6]

Such vulnerabilities could be a result of many factors including inadequate regulations, lack of knowledge of adversary capabilities, incorrect installation and operation of security hardware that do not take into consideration site-specific conditions, or inadequate response strategy and tactics. Often, they could not be uncovered by administrative inspections. For example, NRC inspectors are generally very knowledgeable regarding technical security systems and regulations. They, however, do not have first-hand knowledge of adversary capabilities and tactics, nor do they have specialized training and physical abilities required to test physical security systems against real-world threats.

Many of these problems could be corrected by using the performance-based regulatory approach, which postulates a certain level of security threat (design basis threat) and requires nuclear facilities to demonstrate their ability to defend against this threat. When conducting a performance evaluation, inspectors look at a nuclear facility from the adversary perspective. They then seek to identify its vulnerabilities through systematic and realistic testing.

NRC's first performance testing program was initiated in the early 1980s and was initially intended to evaluate the adequacy of the NRC regulations. Very quickly, however, performance testing has become an important tool for assessing the effectiveness of physical security at individual facilities.

U.S. NRC Performance Testing Programs

The development of a performance-based regulatory approach in the NRC began in the late 1970s/early 1980s. In 1979, the NRC adopted a design basis threat for power reactors, that has since become a foundation of performance testing.[7] Initially, the design basis threat contained two parts: a) an insider in any position, and b) a group of several (specific number is classified) trained and dedicated individuals, which could act in collusion with one insider, and which is equipped with power tools and explosives (to penetrate barriers and damage equipment), and armed with automatic weapons. From the practical standpoint, the lower-level threat represents a disgruntled employee without specialized training. The attributes of the higher-level threat are generally consistent with those of a small group of special forces. In 1994, the design basis threat was expanded to include a car bomb but no performance testing is used to evaluate the plant's ability to defend itself against a vehicle bomb attack; engineering assessment techniques are applied instead.

To conduct performance testing, a specialized team, consisting of a reactor engineer and two security experts, was created in the NRC Office of Nuclear Reactor Regulations. Performance testing calls for unique, interdisciplinary skills. For example, "[A]lthough engineering capability is not unique, its application to safeguards issues requires a broad understanding of physical security, and the ability to view reactor safety systems from the perspective of an adversary."[8] To evaluate tactical response, safeguards specialists must have "operational knowledge of safety equipment and component target sets, knowledge of weapons handling and use in various environments, and tactical approaches that vary based on such factors as plant layout."[9] The team was further strengthened by special contractors with expertise and experience in small group armed combat.

In parallel, a testing program to evaluate vulnerabilities of power reactor equipment to sabotage and to study techniques and capabilities of real-world adversaries was initiated. For this purpose, the NRC procured used and surplus safety equipment (reactor piping, diesel-generators, switchgear, etc.), which sub-

sequently was attacked by explosive devices ranging from a pipe bomb to advanced cutting charges. Similar testing was conducted on doors, fences and other types of barriers typically used in the nuclear power industry to determine their delay value. Testing results demonstrated that without an effective armed resistance terrorists could sabotage a nuclear power plant within three to five minutes after crossing the perimeter line. For barrier penetration and equipment destruction purposes, terrorists would need as little as two to three kilograms of explosives fabricated into specialized charges, not 40–50kg as had been believed.

Since the early 1980s, the NRC has developed two performance testing programs for nuclear power reactors:

- Regulatory Effectiveness Reviews, which in the early 1990s became the program of regional assistance visits; and
- Operational Safeguards Response Evaluations.

These two programs addressed all major elements of a physical security system: access control, detection, assessment, communication, and response and will be described in turn below. Similar programs, for example, Comparability Performance Evaluation Reviews, have been developed for NRC-licensed category I fuel cycle facilities. The U.S. Department of Energy runs performance testing programs to evaluate security at its national laboratories and nuclear weapons production facilities as well.

Regulatory Effectiveness Reviews

The RER program was initiated in 1981 to evaluate the adequacy of NRC regulations and the effectiveness of physical security programs at individual facilities. The program was primarily focused on security hardware, including:

- perimeter intrusion detection and assessment systems;
- access control equipment and operations;
- communication equipment;
- computer systems;
- vital area barriers and access; and
- equipment testing and maintenance programs.

In the late 1980s, the RER program also began to include evaluations of site response capabilities.[10]

A review of a one- or two-unit plant requires five days of systematic evaluation and testing of security hardware and procedures. Most testing is done by special contractors and is based on credible adversary actions and site-specific system weaknesses. The RER staff, in cooperation with other nuclear security specialists, has developed and cataloged a variety of techniques to defeat security systems that are commonly used at nuclear facilities. Many of these techniques, some of which remain classified, require specialized training, equipment, and physical abilities. Performance testing radically differs from operability testing, which is routinely conducted by facility personnel to verify that equipment is operational and meets manufacturer's specifications.

Many weaknesses were identified during the program's early years. At virtually every site, RER team members were able to avoid detection in several of the perimeter's zones. Some examples of generic weaknesses include:

- close proximity of support posts, junction boxes, or fencing to perimeter intrusion detector systems, allowing intruders to jump over the equipment detection zone;
- predictable intrusion pathways via roofs, ledges, etc.;
- vulnerability of assessment systems to alarm stacking;[11] and
- unprotected ventilation openings in vital area barriers.[12]

By mid-1991, all of the operating power reactors had been reviewed and the effectiveness of security systems improved considerably.[13] By that time, for example, even a single successful perimeter penetration had become an extraordinary event. Significant weaknesses, however, remained in the area of armed response. Also, not all plants had been evaluated with respect to their response capabilities. To address these issues and to maintain headquarters' unique inspection program, the NRC management initiated a new program—the Operational Safeguards Response Evaluation—with a focus on contingency response.

Other performance testing functions were folded into regional inspections. Performance testing of security hardware (now called regional assistance—that is, assistance to regional inspectors) is, however, performed by headquarters personnel and special contractors. Regional inspectors are specifically instructed not to conduct performance testing. Regional assistance missions are typically conducted after a licensee has changed or upgraded its security systems, or when a vulnerability is suspected.

Operational Safeguards Response Evaluations

OSRE reviews are designed to evaluate a nuclear power plant's capabilities to respond to an external threat of radiological sabotage. To simplify the analysis, it was decided that OSRE's principal criterion would be reactor core damage (overheating and melting of the reactor fuel), a prerequisite for a massive release of radioactivity from an operating power reactor.[14] From the terrorist standpoint, the objective of an attack then is to eliminate a critical target set—a combination of plant systems and components, such that a combined effect of their destruction would be core damage. Conversely, to prevent core damage, the response forces must be able to protect at least a single element in each of plant's target sets. To achieve this objective, facility's security and operations personnel must identify all critical target sets; establish a correct defensive strategy (duty locations of responders, defensive positions, etc.); be able to execute the defensive strategy; and be able to take appropriate actions to mitigate sabotage damage by manipulating reactor systems. OSRE reviews address each of these elements.

According to the OSRE methodology, an adversary, assisted by a passive insider, has a complete knowledge of facility's target sets, layout, and physical security system. In an overt, over-the-fence assault it attempts to reach a pre-selected set of targets. The adversary uses specialized explosive charges to breach doors and other barriers and to damage reactor's vital equipment. Because of the high speed of attack, off-site assistance is

not available and the plant response forces must be self-sufficient. In order to protect the reactor, the response force must act in such a way as to deploy in a timely manner a sufficient number of adequately armed (typically, with shoulder weapons) and trained responders in prearranged defensive positions. These are the four main criteria used by the OSRE team to evaluate response force performance.

The OSRE team remains on site for five days. OSRE's engineer works with a plant's reactor safety personnel to confirm critical target sets. (Target sets are plant specific and might vary substantially from one plant to another even for reactors of the same type.) The team's safeguards experts receive a briefing on the plant's security program and conduct a facility walk-through to study the plant layout, target locations, and physical protection systems. These data are subsequently used to develop force-on-force drill scenarios.[15]

To evaluate the plant's defensive strategy, the team conducts several table-top drills. These drills represent a tactical chess game, in which OSRE's special contractors play against a security shift supervisor. The game is played on the plant's diagrams and involves moving chess-pieces of responders and terrorists according to the actual time-lines (time intervals required to run from point A to point B).

On-site force-on-force drills are the center piece of an OSRE. The drills (at least four) cover two types of scenarios which are consistent with the NRC design-basis threat: a) a single disgruntled employee with a crowbar, explosives, and a handgun or other weapon, and b) a full-fledged assault by a group of well-armed terrorists. All drills begin at the inner side of the perimeter fence on the assumption that the perimeter detection system performs as intended. A drill ends when terrorists reach a complete target set or when responders neutralize the threat or reliably contain it away from critical targets.

The OSRE team observes but does not actively participate in the drills. It, however, specifies weapons and other attributes of the terrorist group, and designates a target set and a point of entry into the plant's protected area.[16] The role of terrorists is usually played by specially trained officers of the plant's security force. The plant also provides drill controllers to assure safety and to serve as umpires. To increase drill objectivity and realism, many facilities use laser-based simulation, or MILES, equipment. The use of MILES equipment is mandatory at the category I facilities. All drills are videotaped.

In addition to table-top and force-on-force drills, an OSRE includes deadly force interviews with response force members and a technical exchange between OSRE team members and plant's security personnel regarding adversary tactics and capabilities.[17] OSRE's last major element is a firearms demonstration in which response force members must demonstrate tactical and shooting skills in site-specific environments in situations that are likely to occur during an actual attack or have occurred during a drill.[18]

An OSRE concludes with an official briefing for the plant's managers. Upon returning to Washington, the OSRE team writes a report, a copy of which is sent to the licensee. The licensee then has 30 days to respond.

Since the inception of the program in 1991, serious problems have been identified at approximately half of the plants tested. As of May 1999, in more than 40 drills at 27 plants (out of 58 plants reviewed by that time) terrorists were able to reach and destroy critical target sets.[19] Some generic weaknesses include:

- interdiction positions are not appropriate for defending a full range of target sets;
- locations of normal duty stations and equipment storage areas do not allow response personnel to deploy in a timely manner; and
- training programs are not site-specific.[20]

Licensee performance, however, has been improving steadily. Many plants send their representatives to observe OSREs at other facilities and take actions to foresee and address possible concerns. As a result, there is now better coordination between reactor operators and security personnel. More effective defensive strategies have been adopted. For example, many facilities now deploy response personnel inside the reactor and auxiliary buildings, closer to target-rich areas of the plant. Security arrangements have been adjusted (for example, by establishing defensive positions) to accommodate for the OSRE methodology. Table-top drills have become routine and are used widely to strategize response actions. On-site contingency drills are run regularly and their quality has improved. There are better site-specific tactical and firearms training programs.

Making It Work

Performance testing has been critical for improving safeguards and security at nuclear facilities and establishing a meaningful system of regulatory oversight in the United States. Developing and running a performance testing program, however, is not a simple task.

Performance testing is sometimes resented by nuclear utilities because it is perceived as an open-ended process of NRC's imposing increasingly stricter regulatory requirements that are associated with expensive security upgrades. Also, preparations to and hosting of a performance testing inspection in itself could be expensive and disruptive for day-to-day operations.[21] (Nuclear utilities are spending an average of $1.5 million in preparations for OSRE reviews.) Cost considerations are becoming increasingly significant as nuclear power plants now have to compete directly with non-nuclear energy producers due to deregulation. Nuclear utilities consider it a priority to eliminate or minimize costs associated with programs that do not produce kilowatt-hours, including safeguards and security.

Nuclear power utilities are very sensitive to the possibility that performance testing could uncover embarrassing weaknesses that would erode utility's credibility with the public. Some managers are also concerned that poor performance would adversely impact the morale of facility's security personnel and negatively affect their own professional standing.

From the regulatory organization standpoint, performance testing also has its drawbacks. It is more expensive, requires

personnel with unique expertise and backgrounds, and poses a difficult problem of integrating performance testing with baseline compliance inspections. Because performance testing often goes beyond the scope of traditional inspections and can expose weaknesses that are not addressed by the regulations there is a problem of enforcement. Because of relative subjectivity of performance testing and its dependence on expert judgment for the interpretation of test results, disagreements with licensees could be expected and top managers of the regulatory authority must be prepared to deal with disputes.

The following two examples are indicative of potential problems:

In response to the wave of international terrorism in the 1970s, the United States undertook a massive effort to improve physical security at its nuclear weapons production facilities. A part of this effort was the Independent Assessment Program, which was established in May 1979 to conduct independent security evaluations at DOE facilities.[22] The program was created outside of the DOE Office of Safeguards and Security, which has the principal responsibility for nuclear security. The new program was comprehensive in scope and involved some elements of performance testing. For the first time in DOE history, it began using outside experts including representatives from FBI, intelligence community, New York City Police Department, U.S. Army's detachment Delta, and other organizations.

The program identified numerous vulnerabilities at Los Alamos National Laboratory, Savannah River Site, and other weapons production facilities. However, it was terminated in 1981 and a number of its members were transferred to positions unrelated to nuclear safeguards and security (essentially, fired). The principal disagreement within the program and between the program and some sections of the Department of Energy, which eventually led to its downfall, related to the need to evaluate security program management. This caused a problem because, according to some members of the program, "how well the Department's managers were able to meet ...[nuclear weapons] production quotas was used as the predominant measure of the organization's success and the job performance of individual managers. Under this scheme, operating in a safe and secure manner was not allowed to interfere with the primary goal of production. Because security was perceived by these managers as interfering with production, resources that should have been used to improve security were being used to produce more nuclear weapons."[23] (In 1982, the DOE launched its presently operational performance testing program, which is run out of the Office of Security Evaluations of the Office of Deputy Assistant Secretary of Energy for Oversight.)

The second example concerns the Red Cell antiterrorist program.[24] It was started by the U.S. Navy as a classified program in 1985 to test security of U.S. naval installations worldwide. Subordinated directly to the chief of Naval Operations, program staff, mostly counterterrorist experts from the elite SEAL teams, were staging mock terrorist attacks against naval personnel and facilities including nuclear weapons storage areas and strategic submarine bases.

Such testing was very effective in identifying security vulnerabilities to terrorist tactics. The program, however, had been first reduced to table-top drills and, in 1992, was terminated. According to a postmortem analysis by a contractor to the Navy, "There was no demand from the base level. There was no thrust demand from the front level. There was no supply push from the team itself. Those three things coupled with the fairly high cost were enough to kill it. And, as always, there was one precipitating personality who felt it was not cost effective."[25]

NRC's performance testing efforts also have been controversial both in the nuclear industry and within the NRC. For example, some industry representatives have complained at various times that the design basis threat is too high and that OSREs do not take into considerations the operator's abilities to mitigate sabotage consequences. Within the NRC, there have been proposals and motions (eventually rejected or reversed) not to use special contractors, and, even, to phase out OSRE reviews altogether because of limited budgets.

Some experts criticize OSREs as insufficiently stringent and realistic. In particular, it was pointed out that:[26]

- the use of facility's security officers in the role of terrorists can cause a conflict of interests (and, as a result, the use of less-than-professional or unrealistic tactics), and result in inconsistency of testing from one facility to another;
- the assumption about the passive role of an insider is unjustified;
- the number of attackers, as stipulated by the design-basis threat, is unrealistically low; and
- because OSREs are scheduled many months in advance, facility's performance during an OSRE review might be not indicative of its true abilities to defend itself against a terrorist attack.

Despite problems and criticisms, the NRC performance testing programs have been relatively stable and highly effective. Incorrect notions about capabilities of real-world adversaries have been dispelled. Licensees have adopted new and more effective approaches to physical protection. Security personnel have become better trained and equipped, and more professional.

The nature of regulatory activities has also changed. Some elements of performance testing have been integrated into access control, detection, and assessment systems inspections by regional inspectors. Table-top and force-on-force drills are expected to become mandatory, which would institutionalize OSRE-type testing. There are plans to provide training to regional inspectors in the areas of tactical response and performance testing. The NRC management and staff are also discussing possible changes in the 10 CFR 73.55 regulations.

The success of the NRC programs could be attributed to the following factors:

- Program methodology is logical, simple to understand, and addresses real-world vulnerabilities.
- The scope and criteria of performance testing are clearly defined (in part, by the design basis threat) and supported by published regulatory documents.

- The NRC has assembled a team of highly trained and knowledgeable staff. The use of special contractors has also been critical because of their intimate knowledge of adversary tactics and operations, combat experience, and "extensive training and exceptional physical skills."[27]
- The program is transparent to licensee personnel. All testing is conducted in the presence of at least one security officer. Security and facility managers, for example, are briefed daily by OSRE personnel regarding plans and findings. To accommodate production and safety requirements all force-on-force drills are conducted in the evening after the main shift is over.
- Unlike traditional administrative inspections, performance reviews are not conducted on the "pass/fail" basis. The identification of weaknesses is welcome because it helps to make physical security more effective.
- The NRC performance testing programs are supported by NRC commissioners. In addition, the NRC is fully independent from the nuclear power industry and has high credibility with the Congress and the public.

Conclusion

Performance testing is an essential component of an effective, sustainable system of nuclear safeguards and security. The latest revision of INFCIRC/225/Rev.4, the document representing a consensus of IAEA member states regarding physical protection requirements for nuclear materials and facilities, calls for evaluations of technical systems, procedures, and response forces "[T]o ensure that physical protection measures are maintained in a condition capable of meeting the State's regulations and of effectively responding to the design basis threat."[28] Almost 20 years of performance testing in the United States offer valuable lessons on what works and what doesn't work in the world of nuclear security effectiveness evaluations.

Oleg Bukharin is a research staff member at Princeton University's Center for Energy and Environmental Studies. He received his Ph.D. in physics from the Moscow Institute of Physics and Technology. Bukharin conducts research and writes on various aspects of the Russian nuclear weapons program and safeguards and security of nuclear materials and facilities.

Notes

1. The highest level of physical protection is afforded to category I facilities with formula and above quantities of highly-enriched uranium and/or plutonium and nuclear power plants (and some other hazardous fuel cycle facilities), which are protected against theft and diversion of weapons-useable fissile materials and radiological sabotage respectively.
2. For information about the enrichment level of U.S. naval fuel see Albright D., Berkhout F., Walker W. *Plutonium and Highly Enriched Uranium 1996: World Inventories, Capabilities, and Policies,* SIPRI: Oxford University Press, 1997, p. 86.
3. U.S. Code of Federal Regulations: Title 10-Energy; Chapter 1: Nuclear Regulatory Commission; Part 73: Physical Protection of Plants and Materials. (U.S. NRC, reference library, Title 10 of the Code of Federal Regulations; http://www.nrc.gov/CFR.)
4. *Draft: State Concept of Physical Protection,* U.S. Nuclear Regulatory Commission, undated, 9 p.
5. In certain instances, inspections involve physical testing which is conducted in accordance with standard procedures described in NRC inspection manuals and technical documents.
6. Taylor J. *Policy Issue (Information): Regulatory Effectiveness (RER) Program,* SECY-91-052, U.S. Nuclear Regulatory Commission, February 26, 1991, 8 p.
7. Davidson J. and Warren R. "Development and Maintenance of a Design Basis Threat for Use in Designing Nuclear Safeguards," U.S. Nuclear Regulatory Commission internal paper, November 1994, 14 p.
8. Taylor J. *Policy Issue (Information): Regulatory Effectiveness (RER) Program,* SECY-91-052, U.S. Nuclear Regulatory Commission, February 26, 1991, 8 p.
9. Ibid., p. 8.
10. In 1987, the group started conducting table-top drills to assess defensive strategy. In 1988, it began observing force-on-force drills and weapons demonstrations to validate the strategy and assess a facility's tactical response capabilities. Target set reviews were also carried out.
11. "Alarming stacking" refers to near-simultaneous initiation of alarms (most of them false) in different perimeter zones. Because an alarm station operator needs at least several seconds to evaluate and clear away each of the false alarms by using CCTV cameras, an adversary might be able to move past the camera assessment zone by the time the true alarm is being evaluated.
12. *NRC Information Notice No. 88-41: Physical Protection Weaknesses Identified Through Regulatory Effectiveness Reviews (RERs),* U.S. Nuclear Regulatory Commission, June 22, 1988, 3 pp.
13. Taylor J. *Policy Issue (Information): Regulatory Effectiveness (RER) Program.* SECY-91-052, U.S. Nuclear Regulatory Commission, February 26, 1991, 8 pp.
14. In some cases, however, a vulnerability, as demonstrated by RER team members, would be ignored by the facility because it would not constitute a violation of the security plan or regulations.
15. Extensive core damage would likely create a pressure build-up substantial enough to breach the containment of all but the most recent generations of reactors, potentially releasing fission products into the environment.
16. *OSRE Methodology: Evaluation of Contingency Response,* U.S. Nuclear Regulatory Commission, undated, 4 pp.
17. *Operational Safeguards Response Evaluation (OSRE),* NRC Inspection Manual: Inspection Procedure 81110, U.S. Nuclear Regulatory Commission, July 1, 1997, 9 pp.
18. In the United States, the legal standard applicable to law-enforcement and nuclear power plant security issues is that the use of deadly force is appropriate to counter a threat of

death or grave bodily injury to an innocent person. During a deadly force interview, a response officer is presented with a hypothetical scenario and has to make a judgement regarding whether he or she has a legal authority to use deadly force in that particular situation.

19. This could involve shooting from an elevated position (simulating a rooftop or stairwell position), shooting at a moving target, etc.
20. Proceedings of the Briefing on Safeguards Performance Assessment, Public Meeting, U.S. NRC, May 5, 1999; see http://www.nrc.gov/commission/transcripts.
21. Taylor J. *Policy Issue (Information): Office of Nuclear Reactor Regulation (NRR) Safeguards Inspection Activities;* SECY-92-418, U.S. Nuclear Regulatory Commission, December 18, 1992, 5 pp.
22. There are estimates that licensees have been spending from $140,000 to $1.5 million on capital improvements. (see *Testimony of Paul Leventhal on behalf of the Nuclear Control Institute on the Recommendations of the NRC Safeguards Performance Assessment Task Force,* presented to the U.S. Nuclear Regulatory Commission, Washington, DC, May 5, 1999; at Nuclear Control Institute, Current Initiatives, Nuclear Terrorism; http:/www.nci.org/nci-nt.html.) Additional expenses are associated with additional guard training and overtime, and the use of contractors to advise on tactical and training issues.
23. Hnatio J. and Hodges J. *No Second Chance: Conflicting Values Endanger the Security of Nuclear Weapons Activities at the U.S. Department of Energy,* thesis submitted to the School for Summer and Continuing Education, Georgetown University, Washington, DC, April 1992, p. 28.
24. Ibid., p. 40.
25. Cronford S.C. and Wiesman J. (ed.) *Red Cell,* Documentary, L.O.T.I. Group Production, 1993.
26. Ibid.
27. See, for example, *Testimony of Paul Leventhal on behalf of the Nuclear Control Institute on the Recommendations of the NRC Safeguards Performance Assessment Task Force,* presented to the U.S. Nuclear Regulatory Commission, Washington, DC, May 5, 1999. (See: Nuclear Control Institute, Current Initiatives, Nuclear Terrorism; http:/www.nci.org/nci-nt.html.)
28. Taylor J. *Policy Issue (Information): Regulatory Effectiveness (RER) Program.* SECY-91-052, U.S. Nuclear Regulatory Commission, February 26, 1991, p. 6.
29. *The Physical Protection of Nuclear Material and Nuclear Facilities,* Information Circular INFCIRC/225/Rev.4, IAEA, Vienna, Austria.

References

Albright D., Berkhout F., Walker W. *Plutonium and Highly Enriched Uranium 1996: World Inventories, Capabilities, and Policies,* New York: Oxford University Press, 1997, p.86.

U.S. Code of Federal Regulations: Title 10-Energy; Chapter 1: Nuclear Regulatory Commission; Part 73: Physical Protection of Plants and Materials. (U.S. NRC, reference library, Title 10 of the Code of Federal Regulations; http://www.nrc.gov/CFR.)

Draft: State Concept of Physical Protection, U.S. Nuclear Regulatory Commission, undated, 9 p.

Taylor J. *Policy Issue (Information): Regulatory Effectiveness (RER) Program,* SECY-91-052, U.S. Nuclear Regulatory Commission, February 26, 1991, 8 p.

Davidson J. and Warren R. "Development and Maintenance of a Design Basis Threat for Use in Designing Nuclear Safeguards," U.S. Nuclear Regulatory Commission internal paper, November 1994, 14 p.

NRC Information Notice No. 88-41: Physical Protection Weaknesses Identified Through Regulatory Effectiveness Reviews (RERs), U.S. Nuclear Regulatory Commission, June 22, 1988, 3 pp.

OSRE Methodology: Evaluation of Contingency Response, U.S. Nuclear Regulatory Commission, undated, 4 pp.

Operational Safeguards Response Evaluation (OSRE), NRC Inspection Manual: Inspection Procedure 81110, U.S. Nuclear Regulatory Commission, July 1, 1997, 9 pp.

Proceedings of the Briefing on Safeguards Performance Assessment, Public Meeting, U.S. Nuclear Regulatory Commision, May 5, 1999; see http://www.nrc.gov/commission/transcripts.

Taylor J. *Policy Issue (Information): Office of Nuclear Reactor Regulation (NRR) Safeguards Inspection Activities;* SECY-92-418, U.S. Nuclear Regulatory Commission, December 18, 1992, 5 pp.

Testimony of Paul Leventhal on behalf of the Nuclear Control Institute on the Recommendations of the NRC Safeguards Performance Assessment Task Force, presented to the U.S. Nuclear Regulatory Commission, Washington, DC, May 5, 1999; at Nuclear Control Institute, Current Initiatives, Nuclear Terrorism; http:/www.nci.org/nci-nt.html.)

Hnatio J. and Hodges J. 19920 No Second Chance: Conflicting Values Endanger the Security of Nuclear Weapons Activities at the U.S. Department of Energy thesis, Georgetown University, p.28.

Cronford S.C. and Wiesman J. (ed.) Red Cell, Documentary, L.O.T.I. Group Production, 1993.

Testimony of Paul Leventhal on behalf of the Nuclear Control Institute on the Recommendations of the NRC Safeguards Performance Assessment Task Force, presented to the U.S. Nuclear Regulatory Commission, Washington, DC, May 5, 1999. (See: Nuclear Control Institute, Current Initiatives, Nuclear Terrorism; http:/www.nci.org/nci-nt.html.)

The Physical Protection of Nuclear Material and Nuclear Facilities, Information Circular INFCIRC/225/Rev.4, Vienna, Austria: International Atomic Energy Agency, March 1999, p.9.

IAEA's Transportation Burnup Credit Activities

William H. Lake
U.S. Department of Energy
Washington, D.C., U.S.A.

H. Peter Dyck
International Atomic Energy Agency
Vienna, Austria

Note: This paper was presented at the INMM XVIII Spent Fuel Management Seminar, January 12-14, 2000, Washington, D.C.

Abstract

The interests and role of the International Atomic Energy Agency in the use of burnup credit for spent nuclear fuel transport are discussed. Activities of the IAEA related to burnup credit are described. The continuing role of IAEA in this area is addressed. The IAEA burnup credit initiative, which began in 1997, includes observation, assessment, and reporting of international burnup credit activities. Reasons for using burnup credit are presented, along with discussion of general technical and regulatory considerations essential to its use. A worldwide view of the status of international activities on the use of burnup credit for spent nuclear fuel transport is presented, and some specific examples addressed in more detail.

Introduction

Casks used for transport of spent nuclear fuel are approved by national authorities using regulations that are based in varying degrees on the rules developed by the International Atomic Energy Agency. In compliance with these rules, the designer must show that the cask remains subcritical under prescribed conditions of transport (e.g., normal and accident conditions). In the United States, the Nuclear Regulatory Commission promulgates its rules in accordance with the IAEA rules, and publishes them in the Code of Federal Regulations. The NRC's transport regulations are found in 10 CFR Part 71.

Until recently, in all parts of the world, criticality safety analyses, done to demonstrate subcriticality under transport conditions, assumed that the SNF was in its most reactive state. That is, the SNF was assumed unburned. The advantage of this fresh fuel assumption is simplicity. The disadvantage of the fresh fuel assumption is unnecessary inefficiency and the need for criticality controls that are more than needed to maintain subcriticality when one considers the actual physical state of the SNF. These unnecessary controls result in additional shipments and expensive control devices. More shipments increase worker and public exposures, risks (both radiological and non-radiological), and costs. Although exposures and risks from transport are small, any avoidable increases are undesirable.

The practice of accounting for the true state of SNF is known as burnup credit. This departure from the relative simplicity of the fresh fuel assumption for demonstrating criticality safety raises a number of technical and regulatory challenges for the design and use of casks that use burnup credit. The design challenges include knowledge of the irradiation history of the SNF, isotopic concentrations, and physical characteristics of the isotopes affecting criticality. In addition, the analytic tools used to predict isotopic concentrations (e.g., depletion codes) and to demonstrate subcriticality (e.g., criticality codes) must be extended and proven for use of SNF in transport casks. The regulatory challenge includes demonstrating the ability to use the available data and tools to assure subcriticality. It is worth noting that neither the IAEA rules nor the NRC rules prohibit the use of burnup credit. Therefore, the use of burnup credit does not require any change to the rules and regulations that control SNF transport.

The principal operational challenge associated with the use of burnup credit is that of assuring that the SNF loaded into a burnup credit approved cask meets the design load specifications. It is generally believed that reactor records may be sufficient for that purpose, but physical measurements have been required for current and pending approvals (e.g., France and the United States). Although this redundancy is likely to continue for some time, many believe that this practice can be relaxed as operating history is gained and sufficient confidence in reactor records and the effectiveness of administrative controls is achieved.

The IAEA recognized the importance and worldwide interest in the use of burnup credit for spent fuel management systems, and in 1997 convened a consultants meeting to explore the sub-

ject. The consultants concluded that there was sufficient worldwide interest in using burnup credit to justify further consideration by IAEA. The Agency decided to hold an advisory group meeting to determine the extent of that interest and the level of progress. The Advisory Group Meeting was held in Vienna, Austria during Oct. 20-24, 1997. The Proceedings of the AGM was published in April 1998.

The participant countries and organizations of the 1997 AGM are described. The technical and related regulatory findings of the AGM are discussed briefly. The transport burnup credit activities, which were reported in the Proceedings of the 1997 AGM, are summarized. Where information is available to the authors, significant progress since 1997 is described. The situations in France and the United States are discussed in more detail.

France is an interesting case because their industry and regulatory authorities can pride themselves on developing and issuing the world's first approval of transport burnup credit. The use of burnup credit for SNF transport has been going on for some time in France. France was motivated to use transport burnup credit to maintain capacities of its existing cask fleet as initial enrichments of fuel were increasing. France is representative of countries with mature nuclear programs that use reprocessing. The situation in the United States is of interest to an American audience, but further, it is representative of countries that have committed to direct disposal of SNF and are currently storing SNF at or near reactor sites.

The IAEA Advisory Group Meeting of 1997

Fourteen countries and one international organization in addition to the IAEA participated in or contributed to the 1997 AGM proceedings. The countries included Bulgaria, Czech Republic, France, Germany, Hungary, Japan, Republic of Korea, Russian Federation, Slovakia, Spain, Sweden, Switzerland, the United Kingdom, and the United States. The other international organization that joined IAEA in the AGM was the Organization of Economic Cooperation and Development, Nuclear Energy Agency. OECD/NEA described its ongoing activities in developing benchmarks for criticality safety analysis.

The 1997 AGM addressed the use of burnup credit for wet and dry storage, transport, reprocessing, and disposal of SNF. The fuel types considered by the group included boiling water reactor fuel, pressurized water reactor fuel, mixed oxide fuel, Wodo Wodyanoi Energetichecki Reactor (WWER) fuel, and RBMK fuel. WWER is a Russian-type PWR, usually referred to in the West as VVER, a designation that will be used in this paper. RBMK is also a Russian reactor design. A look at the AGM proceedings suggests that the most active area for burnup credit is SNF storage. Wet storage burnup credit was generally pursued first as a means of increasing pool capacity. Once pools were filled, those needing additional SNF storage would turn to dry systems. As dry storage technologies mature, burnup credit is being used, pursued, or considered to improve dry storage efficiencies. Storage of SNF is an issue that currently confronts most, if not all, countries with nuclear power generating capability. An IAEA symposium addressing the important subject of SNF storage was held in November 1998.

The use or development of burnup credit for reprocessing and disposal of SNF is limited to the countries that have committed to either of these specific types of fuel cycle. It was found that many countries had not committed to a specific fuel cycle, choosing instead to follow a wait-and-see policy. Of the reprocessing countries, France was using burnup credit, while Japan, Russia, and the United Kingdom were in various stages of development. Of the countries planning to dispose SNF, Czech Republic, Germany, Slovakia, Sweden and the United States were in various stages of consideration or development of using burnup credit for their disposal strategies.

Most countries could see the benefits of using burnup credit for transport; however, unlike storage, the need for burnup credit for transport of SNF was found less urgent. Consequently, progress in transport burnup credit is not as advanced as it is in storage applications. France was already using burnup credit for PWR SNF transport at the time of the 1997 AGM, and Switzerland, using French casks and reprocessing capabilities honored the French approval for transport in Switzerland. Germany, Japan, Russia, the United Kingdom, and the United States had active development programs, with the UK and United States having dialogue or applications before their regulatory authorities. In addition to Russia's interest in using burnup credit for SNF transport, other Eastern European countries participating in the AGM expressed their interest. These countries, which include Bulgaria, the Czech Republic, Hungary, and Slovakia, all use the Russian designed VVER. The RBMK reactor designs are also used in the Eastern European countries, and burnup credit is sought for storage applications, but not for transport.

IAEA's Continuing Role

The Agency convened a number of consultants meetings subsequent to the 1997 AGM. Tasks assigned to the consultants on the implementation of burnup credit included assessing the value of the AGM, determining if the Agency should establish a continuing role in the area of burnup credit, and if so, recommending what that role should be.

In their assessment, the consultants concluded that the Agency's burnup credit activity had been beneficial to the participants, and to other interested parties, through the general availability of the proceedings of the 1997 AGM. The consultants concluded that the document provides a comprehensive discussion of burnup credit, the motivations for its use, regulatory status, current practice, planned activities, analytic tools, parameters affecting burnup credit, criticality safety, operational practices and verifications, and data needs. The proceedings were characterized as a baseline for burnup credit.

The consultants noted the dynamic nature of the national burnup credit programs, observed progress, commonality of issues, and similarities in resolutions for the issues identified. The consultants suggested that because of those factors, a focused forum for an exchange of technical views, information, and data was beneficial. The consultants agreed that the IAEA

activity had provided such an opportunity, and should continue while burnup credit activities continue to progress at the current rapid rate. The consultants further recommended that the need for continuance of the Agency's activities in this area be addressed on a regular basis.

The consultants recommend that the direction of the Agency's continuing burnup credit activities follow the current needs of those involved in spent fuel management. That is, the activities should be sensitive to evolving needs. It was further observed by the consultants, that a major activity, important to the use of burnup credit, was already being handled effectively by the OECD/NEA. That is, the benchmarking of computational methods and development of experimental databases used for criticality safety analysis. The consultants advised that IAEA activities focus on the practical implementation of burnup credit for spent fuel management systems. The consultants further observed that the Agency's work on implementation of burnup credit for spent fuel management systems was complemented by the OECD/NEA work already accomplished. As OECD/NEA continues to perform its activities to support continued progress in burnup credit analysis, those efforts should be considered by the Agency in planning its future activities in the area of implementation of burnup credit.

The next major burnup credit activity planned by the Agency will be a *technical committee meeting* planned for the summer of 2000. The TCM will be convened as a forum of representatives from countries and international organizations having interest in using burnup credit for spent fuel management activities. Participants will be asked to describe national programs and to address technical and regulatory matters that pertain to the various applications of burnup credit. The TCM will expand the participation of the AGM by inviting additional countries and more representatives from each country. National authorities from countries offered an opportunity to participate will select appropriate experts as representatives. Representatives to a TCM who are selected by national authorities, generally, must seek their own funding for TCM participation. Although the TCM participants will be limited to selected experts, the proceedings will be published and generally available to interested parties within one year of the TCM.

Technical and Regulatory Considerations

Consideration of the contributed papers from the 1997 AGM participant countries on their respective national burnup credit programs suggested a common understanding of the important technical issues on the subject. These commonly acknowledged issues are described in this section.

A substantial amount of data and experience exists for demonstrating criticality safety for transport casks using the fresh fuel assumption. This information, supplemented with additional technical data specific to burnup credit, provides a foundation for developing a technical basis for using burnup credit.

Computer programs are available to predict isotopic inventories for spent fuel and to perform criticality safety analysis for casks containing SNF. Although these analysis tools are used with confidence for many applications, using them for demonstrating criticality safety for transport casks using burnup credit is a new endeavor that may require additional justification.

Depletion codes are used routinely for reactor core analyses, and isotopic prediction for shielding safety analyses for transport casks. However, for demonstrating criticality safety for transport casks that use burnup credit, additional chemical assay data may be needed to benchmark these computer codes. The assay data should be developed with sufficient precision to support the level of credit that is given for burnup. It should include all fissile elements and any neutron absorbing actinides and fission products that will be considered when using burnup credit. Since the fissile isotopes all contribute to reactivity, none should be ignored. However, any of the non-fissile actinides or fission products, which are neutron absorbers that decrease reactivity, may be ignored. The choice of which neutron absorbers to include and which to ignore is generally dictated by balancing the difficulty of obtaining the necessary nuclear data and the benefits derived in terms of negative reactivity available from the isotopes of interest.

Additional benchmarks for computer codes used for criticality analysis of burnup credit casks may also be needed. A number of fresh fuel critical experiments are available and have been used to validate many of the computer codes used in countries that participated in the 1997 AGM. These benchmarks could be applicable for criticality analysis of systems using burnup credit. These experiments address the fissile uranium concentration for fresh fuel (i.e., U-235) and the effects of materials of construction and geometry for SNF transport casks. There are also a number of experiments performed on MOX fuel, which may be applicable to the actinide-only burnup credit method. The MOX experiments would provide data on the fissile actinides and various actinide absorbers present in spent fuel. However, additional experiments may be required. For fission products that might be considered for burnup credit, appropriate benchmarks are likely to be needed. Because these effects can be treated independently, a set of isotope specific experiments can be used to account for the variables of interest for burnup credit.

The OECD/NEA reported on the ongoing international benchmarking activities at the 1997 AGM. The OECD/NEA activities are being conducted to benchmark computer codes for use in transportation SNF burnup credit applications. The effort, which began in the 1980s, continues to compile sets of benchmark problems that have been devised, solved, reviewed, and resolved by a group of international criticality safety experts. The work of the OECD/NEA benchmarking group is essential to those engaged in computer code validation.

A characteristic of spent fuel that is important to criticality safety is the axial distribution of burnup. For PWR and VVER reactors, which are controlled by boron in a water solution, the axial distribution of burnup exhibits a high degree of uniformity over the central region. Because of the higher neutron leakage at the top and bottom ends of a reactor core, fuel assemblies

tend to be less burned in these regions. The resulting increased reactivity at the ends is the so-called end-effect. This is not a factor for the fresh fuel assumption, since all fuel is assumed unburned; however, it is a factor for SNF.

Using the fresh fuel assumption requires assurance that any SNF fuel loaded into a transport cask meet the fuel specifications that pertain to criticality safety. These specifications are the initial enrichment and identification of the fuel design. Assurance of proper cask loading for the fresh fuel assumption is done using administrative controls. For casks using burnup credit, an additional factor must be considered. That is, burnup must meet the minimum burnup required for the fuel's initial enrichment. The operation of a nuclear reactor requires the collection and retention of operating data, which includes burnup history. Many believe that this data is adequate to assure identification and proper loading of the SNF into a cask that uses burnup credit. Current regulatory practice is to provide additional verification of SNF burnup levels for loading into a cask that uses burnup credit. Verification of the SNF burnup, which is determined from reactor records, can be done by a measurement of a predictor of burnup.

Transport Burnup Credit Programs—Worldwide

Although there is considerable worldwide interest in using burnup credit for SNF transport, progress seems to be concentrated in a few countries that have large nuclear programs. Western Europe, France, Germany, and the United Kingdom are using burnup credit for transport, or are in advanced stages of development. In Eastern Europe, the Russian Federation is using burnup credit for SNF transport. In Asia, Japan has an active development program underway. In the Americas, the United States has been actively pursuing burnup credit for SNF transport. The 1997 AGM participants found that actinide-only approaches for transport burnup credit were used as a starting point. Actinide-only burnup credit considers the fissile actinides and selected neutron absorbing actinide isotopes. Most countries considering the use of actinide-only burnup credit, however, had plans to extend that credit to include credit for selected sets of fission products.

Western Europe

France, the first country to begin routine use of burnup credit for SNF transport, has been doing so since the late 1980s. The current approval in France is for actinide-only for PWR SNF.

Germany is interested in burnup credit, and has a number of burnup credit activities currently underway. In particular, these activities include wet storage and dry transport applications of burnup credit. Germany has abandoned a policy of domestic reprocessing of SNF. In the absence of reprocessing, Germany will likely adopt a burnup credit implementation strategy similar to that of the United States.

Spain has approved burnup credit for wet storage of PWR and BWR spent fuel. Spain also has interest in using burnup credit for dry storage and transportation applications (dual-purpose systems).

Sweden has approved the use of burnup credit for wet storage of BWR spent fuel and is beginning to develop burnup credit data for disposal of spent fuel. Sweden is also interested in using burnup credit for dry transport systems.

Switzerland allows the use of burnup credit for French approved dry PWR spent fuel transport under international agreements. Switzerland is also interested in burnup credit for dry transport of BWR and MOX spent fuel.

The United Kingdom does not currently use burnup credit for their existing fleet of water cooled casks, but anticipates having to use it in the future to avoid reducing existing cask capacities as initial enrichments of new fuel designs increase. Since the 1997 AGM, cask developers in the UK have submitted a reference case to the regulatory authorities. The UK has an active reprocessing program, and will likely develop a burnup credit implementation program similar to the French program.

Central and Eastern Europe

The Eastern European countries participating in the AGM (i.e., Bulgaria, the Czech Republic, Hungary, Russia, and Slovakia) all use the Russian designed VVER, which is similar to the PWR, but with a hexagonal fuel arrangement. All have interest in storage and transport applications for burnup credit. Russia is also interested in reprocessing applications. Before the dissolution of the Soviet Union, the Russian Republic supplied the other republics and Eastern European countries with nuclear power technology. Now each country is responsible for its own technology development. Although there appears to be considerable economic benefit available to these countries from using burnup credit for their VVER systems, the cost of developing the technology may frustrate their efforts.

Asia

Japan has a sizable nuclear program, and those involved in nuclear power have considerable interest in the possibility of using burnup credit for SNF management applications. Japan is interested in storage, transport, and reprocessing applications, and is engaged in a variety of research and development activities related to burnup credit. Although Japan's R&D efforts are extensive, and burnup credit is used for storage, the pursuit of burnup credit for SNF transport has not reached the regulatory review stage, which is a necessary step toward implementation. The Republic of Korea has a smaller program than that of Japan. ROK already uses burnup credit for wet storage of PWR spent fuel, and is interested in using it for transportation.

The Americas

The United States is the only country in the Americas developing burnup credit technologies. The United States plans to use burnup credit for SNF shipments from about 100 nuclear reactors to a repository for deep geological disposal. The shipments to the disposal site are expected to begin by 2010. The U.S. effort was initiated by the Department of Energy in the mid-1980s. The DOE, which led this effort until 1998, submitted a topical report for actinide-only PWR burnup credit to the NRC in 1995 [DOE, 1995]. Following NRC reviews of the report,

two revisions were submitted in 1997 and 1998 [DOE 1997, 1998]. In 1999, NRC issued guidance for the use of burnup credit for SNF transport [NRC, May 1999, August 1999].

A Closer Look at Burnup Credit Activities in France and the United States

France leads the world in implementing burnup credit for transport of spent fuel. The French have been using an actinide-only approach for transportation burnup credit and reprocessing activities since the late 1980s. Their approach is conservative, but completely serves their needs, which for transportation, is to continue the use of existing, multi-element casks at full capacity, even as initial enrichments of new fuel designs increase. A significant conservatism of the French approach rests in the assignment of assembly burnup, which uses the average burnup of the first 50 centimeters for the assembly. The approach, which credits less than about two-thirds to three-fourths of the assembly average burnup, provides a large criticality safety margin. Furthermore, by basing the credit used on the underburned ends, the issue of end effects is inherently addressed by the method.

France is currently developing critical benchmark data to extend the approval for SNF transport burnup credit to include consideration of fission products. The initial approach is expected to consider a limited number of fission products (i.e., six) that account for approximately 50 percent of the available fission product burnup credit. Plans are also being developed in France to gather additional data to expand the set to include 12 to 14 fission products.

The United States is seeking burnup credit for PWR SNF transport. The U.S. program has not achieved the regulatory success that France's has. A contributor to that fact may be that the U.S. program is more aggressive with regard to the amount of credit sought. The United Sates is initially seeking actinide-only burnup credit for a full range of initial enrichments; however, it desires more credit for the available spent fuel burnup (e.g., using assembly average burnup with correction for end effects). The motivation that led the United States to seek burnup credit is different from that of France. While France was motivated by the desire to continue using existing casks at rated capacity, the United States seeks to develop new casks with the highest achievable capacities.

The United States is developing a repository for deep geological disposal of SNF. While a repository is being developed and licensed, SNF is stored at about 100 reactor sites throughout the United States. When a repository begins accepting SNF for disposal, currently expected by 2010, a major 30-year shipping activity will begin. Estimates indicate that cask capacity increases of 30 percent can be achieved for current generation rail casks that use burnup credit. A truck cask approved by the NRC in 1998 that was designed as a burnup credit cask will carry four PWR SNF assemblies over a full range of initial enrichments when burnup credit is used. The same cask is limited to two assemblies for higher initial enrichments when burnup credit is not used. Although the NRC has issued guidance on using burnup credit, they have yet to receive certification applications for its use. However, several vendors with canister-based rail casks have indicated plans to submit a request for burnup credit in the near future.

An interesting situation in the United States is the increased development and use of dual-purpose canister-based cask systems. The canister-based system uses a common canister for storage and transport. The canister is designed to fit into appropriate cask systems for storage and transport. The advantage of the dual-purpose system is the minimization of fuel handling. Ideally, the canister is loaded before storage, and shipped off site without repackaging when the storage period at the reactor site ends. The complication that arises is the fact that burnup credit-like loading configurations can be achieved for canister-based storage of SNF. However, if the canister-based dual-purpose cask is not approved for transport burnup credit, it must be opened and repackaged prior to transport. Since these systems are being implemented now for storage at reactor sites, use of the more efficient burnup configuration risks the need to repackage prior to transport.

Conclusions

Based on ongoing international activities, it is evident that the use of burnup credit for demonstrating criticality safety for SNF management has gained worldwide interest. Burnup credit is recognized as a means of increasing efficiency not only for transportation, but also for storage, reprocessing, and disposal of SNF. There has been considerable progress in the use of burnup credit for SNF transport applications since the IAEA held its 1997 AGM. Because of the dynamic nature and rapid progress in burnup credit activities worldwide it is beneficial to have an established forum where information and ideas on the general use of burnup credit can be discussed and exchanged. The IAEA is ideally suited to this role and has accepted that responsibility, which will continue as long as appropriate. Toward that end, the proceedings of the 1997 AGM, which serves as a baseline for worldwide burnup credit activities, will be supplemented by the proceedings of a TCM, expected to be issued by 2001.

Although the greatest need and most activity in burnup credit continues to focus on SNF storage, increased attention is being observed in transport applications. The two examples cited in the paper show different facets of the same goal, the use of burnup credit for efficiency in SNF transport.

In the case of France, shipments of short cooled SNF, destined for reprocessing plants are shipped using an established fleet of multi-assembly casks. The use of fuel with higher initial enrichments to improve efficiency for nuclear power generation, threatens the capacities of these casks. Burnup credit has been found as an effective means of maintaining capacities of the casks, even as initial enrichments continue to rise. The second case considered is the United States, where a new generation of casks is being developed to handle older, long cooled fuel destined for deep geological disposal. The goal in this case is to develop casks with maximum capacity ratings for a range

of initial enrichments that envelope those available now, and those expected in the future. Although somewhat different, both situations require the same technical data, tools, and methods. Both encounter similar regulatory issues. Furthermore, the argument of commonality of technical and regulatory information extends to all potential users of burnup credit. Since the objective of using burnup credit is to improve efficiency, extending the objective to technology development is suggested. The development of burnup credit technology is expensive, and because the basic data and tools may have broad application, cooperation and exchange is clearly indicated. This is an effort supported and encouraged by the IAEA.

References

Department of Energy, *Topical Report on Actinide-Only Burnup Credit for PWR Spent Nuclear Fuel Packages,* May 1995 (DOE/RW-0472 Rev. 0).

Department of Energy, *Topical Report on Actinide-Only Burnup Credit for PWR Spent Nuclear Fuel Packages,* May 1997 (DOE/RW-0472 Rev. 1).

Department of Energy, *Topical Report on Actinide-Only Burnup Credit for PWR Spent Nuclear Fuel Packages,* September 1998 (DOE/RW-0472 Rev. 2).

International Atomic Energy Agency, *Regulations for the safe transport of radioactive material*—1966 Edition, Safety Standards Series ST-1/Requirements, STI/PUB/998, Vienna, Austria (1996).

International Atomic Energy Agency, *Storage of spent fuel from power reactors,* Proceedings of an Advisory Group meeting held in Vienna, 20-24 October 1997, IAEA-TECDOC-1013, Vienna, Austria (April 1998).

International Atomic Energy Agency, *Implementation of burnup credit in spent fuel management systems,* Proceedings of a Symposium held in Vienna, 9-14 November 1998, IAEA-TEC-DOC-1089, Vienna, Austria (July 1999).

U.S. Nuclear Regulatory Commission, Title 10 Code of Federal Regulations (CFR) Part 71, 1999.

U.S. Nuclear Regulatory Commission, Spent Fuel Project Office, Interim Staff Guidance - 8, Limited Burnup Credit, ISG-8, May 17, 1999.

U.S. Nuclear Regulatory Commission, Spent Fuel Project Office, Interim Staff Guidance, ISG - 8, Revision 1, Issue: Burnup Credit in the Criticality Safety Analyses of PWR Spent Fuel in Transport and Storage Casks," August 8, 1999.

Spent Fuel Storage Developments in Eastern Europe and Former Soviet Union

F. Takáts
TS ENERCON KFT
Budapest, Hungary

H. Peter Dyck
IAEA
Division of Nuclear Fuel Cycle and Waste Technology
Vienna, Austria

Note: This paper was presented at the INMM XVIII Spent Fuel Management Seminar, January 12-14, 2000, Washington, D.C.

Abstract

There are 81 nuclear power plant units in the former Soviet Union and in Eastern European countries, with a generating capacity of more than 50,000 MWe. Changes in politics and trading relationships are affecting spent fuel management policies. This paper describes the various approaches to the back-end of the nuclear fuel cycle adopted in these countries and reports data on the amount of spent fuel discharged from the nuclear power reactors with a summary table. Various types of interim storage facilities under consideration are described with a table for the Away-From-Reactor spent fuel storage capacities for the countries of the former Soviet Union and Eastern Europe.

History

In the 1970s, the Soviet Union and almost all Socialist countries in Europe launched an extensive nuclear program. They constructed mostly WWER type units. Typically each unit has a spent fuel storage pool, with a capacity to store the discharge of at least three years' operation and a full core reserve in a so-called reserve rack. Such power stations were constructed in the following countries, which were outside the Soviet Union: Bulgaria, Czechoslovakia, the German Democratic Republic, and Hungary. One power generator from Finland (Imatran Voima - IVO) also built two units at the Loviisa site. Poland and Romania started the construction of WWER units, but the work was stopped at one stage.

In those years, fuel cycle cost calculations contained a high credit for the plutonium and uranium residual in the spent fuel. Thus it was clearly an asset bound for recycling, after decay cooling, and the availability/guarantee of reprocessing was never questioned. Technologies were developed for the transport of spent fuel. The COMECON countries involved all signed the international agreement on regulations for the transport of spent fuel by rail or ship.

At a request of the Soviet government nuclear power plants were required to provide at least five years cooling of spent fuel before dispatching it for reprocessing. As an interim measure, many countries constructed wet storage facilities with 600 tHM capacity. Such Away-From-Reactor facilities were constructed in Bulgaria, Czechoslovakia, the GDR, and at some power plants of the Soviet Union. IVO of Finland constructed a pool storage system of its own design. Hungary investigated the available options and simply reracked the at-reactor storage pools.

Nuclear Power Plant and Spent Fuel Data

Number of nuclear power plants

Altogether 79 nuclear power plant units of the Soviet design were constructed in the former Soviet Union and in the countries of Eastern Europe, with a generating capacity more than 50,000 MW_e. Sixteen units were shut down, and/or are being decommissioned. Six units are being decommissioned in Germany, one unit is shut down in Armenia, Kazakhstan, and Slovakia respectively. Three units of Chernobyl do not generate any more spent fuel. Eight more Soviet-designed units are under construction or being commissioned in the Czech Republic, Russia, and the Ukraine.

Romania operates a CANDU unit. There are two more countries to be mentioned: Finland and Slovenia. The Loviisa nuclear power plant in Finland has two WWER-440 units. Slovenia, which belongs to the geographic region, has a single-unit nuclear power plant supplied by Westinghouse.

The breakdown by countries and unit types is shown in Table 1.

Spent fuel data

A typical WWER-440 unit discharges about 120 spent fuel assemblies, a WWER-1000 about 55 assemblies, and an

Table 1

Country	Type of Reactor	Number of Units	Remarks
Armenia	WWER-440	2	One unit is shut down.
Bulgaria	WWER-440	4	In operation.
	WWER-1000	2	In operation.
Czech Republic	WWER-440	4	In operation.
	WWER-1000	2	Under construction.
Finland	WWER-440	2	Altogether, four in the country.
Germany (Former GDR)	WWER-70	1	All six units to be decommissioned.
	WWW-440	5	
Hungary	WWER-440	4	In operation.
Kazakhstan	BN-350	1	Shut down and defuelled.
Lithuania	RBMK-1500	2	In operation.
Romania	CANDU-600	1	In operation.
		3	Under construction.
Russia	RBMK-1000	11	In operation.
	RBMK-1000	1	Under construction.
	BN-600	1	Fast breeder.
	EGP-12	4	Small heating plants, shut down.
	WWER-440	6	In operation.
	WWER-1000	7	In operation.
	WWER-1000	1	Under construction.
	BN-800	2	Fast breeder, under construction.
Slovakia	A-1 (HWGCR)	1	Being decommisioned
	WWER-440	6	In operation.
Slovenia	Westinghouse PWR	1	In operation.
Ukraine	RBMK-1000 Chernobyl	1	In operation.
		3	Shut down.
	WWER-440	2	In operation.
	WWER-1000	10	In operation.
	WWER-1000	2	Under construction.

RBMK-1000 about 450 assemblies each year.

The weight of one year's discharge is:

- 14 tHM for a WWER-440 unit;
- 25 tHM for a WWER-1000 unit; and
- 58.5 tHM for an RBMK-1000 unit.

The spent fuel inventories in the countries are shown in Table 2.

The at-reactor storage pools of the power plants are usually filled to their design capacity. As mentioned above, some countries constructed a wet AFR storage facility. These buildings consist of four storage pools (one of them is reserve), and the necessary cask unloading, water cooling, filtering, etc. services. Spent fuel is stored in the baskets that are used also during transportation, i.e., the fuel itself is not handled directly after loading of the basket. At all RBMK plants similar storage units exist.

Table 2

Spent fuel inventory in the Eastern-European countries, in the Soviet-made power reactors of Finland, Germany and in the Republics of the former Soviet Union (tHM) in 1999.

Country	AR	AFR	Total in Country
Armenia	95	-	95
Bulgaria	461	357	818
Czech Republic	281	333	614
Finland	264	715	979
Germany	34	571	605
Hungary	348	134	482
Kazakhstan	0	15	15
Lithuania	1,421	29	1,450
Romania	186	-	186
Russia	2,945	8,639	11,584
Slovakia	136	570	706
Slovenia	215	-	215
Ukraine	1,739	1,743	3,482
Total	**8,125**	**13,106**	**21,231**

In those countries, that do not have such wet storage facilities or where they are reaching the design capacity, new AFR facility projects are being reviewed or actually constructed. All these new designs use the dry storage principle. Four countries decided to construct metal cask storage, one country selected the NUHOMS design, another the Modular Vault Dry Store System, and one nuclear power plant chose the VSC design. The selection by the electric utility of a dry vault design has been announced for two RBMK plants, but the final decision is delayed. Further decisions can be expected the near future. For some countries, which already have selected one mode of storage, the further extension can be different from the type previously selected.

Spent Fuel Management Approaches

The collapse of the Soviet Union and changes in the politics and trading relationships of the newly formed states also affected their spent fuel management policies. Russia now requires payment for the services in hard currency at a world market price level. There are also some legal problems with the licensing of spent fuel transport through the newly formed states, and the subsequent reprocessing in Russia. A decree was adopted in Russia in 1993 which forbids the import of radioactive wastes from abroad, but the question, as to whether spent fuel is waste or not, is still being challenged. Since the introduction of the new prices, only Finland and Hungary have signed contracts for spent fuel reprocessing services, but both countries stopped sending their spent fuel to Russia. Bulgaria is trying to license shipments to Russia, because the pools at Kozloduy are reaching capacity, and Slovakia sent all fuel from the A-1 reactor back to Russia. Two former Soviet states—Armenia and Ukraine—were also able to ship some spent fuel back to Russia under special conditions.

These are the main factors, which led to changes in the spent fuel management policy of these countries. At least six of the countries involved have plans to develop direct disposal, while the others are delaying the decision.

Armenia

Only one reactor is in operation presently. Due to the unavailability of nuclear fuel reprocessing or a permanent geologic repository in Armenia, the pool of the operating facility is full, and the full core reserve has been used. The pool of the shut down reactor (Unit 1) is also full.

An interim storage facility using the NUHOMS system supplied by FRAMATOME has been chosen for the Medzamor site. As the number of assemblies to be stored in one module is 56, the model type is designated NUHOMS®-56V.

To enable the storage of 612 assemblies, construction of 11 horizontal storage modules has been decided. The 11 HSM are grouped together to form two arrays of respectively five and six HSM. The two arrays are arranged back to back.

The criticality analysis performed for the NUHOMS-56V DSC fuel does not account for fuel burnup but takes credit for soluble boron and demonstrates that fixed borated neutron absorbing material is not required in the basket assembly for criticality control. This solution and some other issues have encountered a number of licensing problems. It is expected that the issues will be resolved and fuel can be loaded in the first modules very soon.

Bulgaria

Bulgaria has an AFR(RS) wet storage facility on the site of the NPP Kozloduy. The capacity of the AFR facility is 600 tHM. It is in the process of renovation to meet current seismic standards. Bulgaria considered developing a dry storage facility, but postponed that decision after deciding to rebuild the wet facility.

Proposed in 1974 as an alternative to spent fuel transportation to the USSR, construction of Kozloduy AFR(RS) facility

did not begin until 1982. The first fuel receipts to this facility were made in February 1990.

The facility was the first of a proposed common design for an AFR at the Soviet built reactors to store WWER fuel and it comprises fuel receipt, unloading and storage areas. The current design is slightly different from the other facilities because this was meant for the long-term storage of 168 baskets (4,920 assemblies, ~600 tHM) of spent fuel from the sites four WWER-440 and two WWER-1000 reactors; to be loaded over a period of 10 years.

After cooling for three years in the AR storage pools, the assemblies are transported to the AFR(RS) by an on-site transport container and a specialized trailer unit. Yearly receipts are at the rate of 25 transport baskets comprised of four baskets or 120 fuel assemblies per WWER-440 reactor and nine baskets or 108 fuel assemblies from the two WWER-1000 units.

The storage area is made up of three operational water bays and a contingency bay to allow for preventive maintenance/provision against major in-bay failure. The storage bays can be isolated from each other by hydraulic seals/gates for repairs. All pools are doubled lined with carbon and stainless steel.

Czech Republic

The pool storage capacity at Dukovany Power Station was expanded almost twofold relative to the original design by reracking.

A dry cask storage facility using CASTOR casks is in operation at the site of the NPP. The dry storage facility is now more than half full. An extension of this facility by another 60 casks (600 tHM) is under discussion. The interim storage will have a design life of up to 50 years.

The construction began in June 1994 and was completed in October 1995. The first CASTOR 440/84 cask was loaded in November 1995.

The facility is licensed to store up to 60 CASTOR 440/84 casks. The capacity of each cask is 84 assemblies or approximately 10 tHM. Spent fuel characteristics for the CASTOR 440/84 include: storage of WWER 440 spent fuel; 35,000 MW d/tHM burnup; 3.5 percent 235U enrichment; a minimum fuel age of 5 years prior to storage; no damaged assemblies may be stored; maximum cladding temperature of 350°C. A Tender Invitation to supply the next 60 metal casks has been issued.

The storage building has a cask receiving area, which is separated from the storage area by a concrete shielding wall. This wall is approximately 40 cm thick and 6 m high except for a center 4.5 m high section over which the cask is lifted when being moved from the receiving area to storage area. The floor of the storage building is a reinforced concrete plate. The building has one hall with columns and a light steel roof. The columns support an overhead rail for the 130-ton crane. The external walls of the storage building were constructed with ordinary concrete and brick wall panels. The removal of the decay-heat is achieved by natural convection through openings in the side walls and the roof of the storage building.

Finland

Because of the special construction of the reactor containment at Loviisa, the AR pools are somewhat smaller, and the first phase of an AFR wet store was constructed in 1980, even though spent fuel was still shipped back to the Soviet Union (Russia), until 1996. A second phase was constructed in 1984.

Phase 1 of the Loviisa AFR(RS) was brought into operation in 1980, increasing the storage capacity of the unit 1 NPP to take account of a need for increased fuel cooling from three to five years prior to transport for reprocessing in the Soviet Union. The AFR facility was extended later in 1984 (phase 2) to provide additional storage capacity for unit 2 of the NPP.

The two phases of the AFR facility were built alongside one another three meters below ground. The services for each phase are provided by the associated unit of the NPP.

Phase 1 comprises two parallel storage bays, a loading bay, a decontamination well for casks, a dry disposal area for control rods, and a covered deck under which the cask transport vehicles are located. The storage bays are connected to the loading bay by gates and each bay has a capacity for up to eight fuel baskets. A fuel basket can accommodate 30 fuel assemblies with a hexagonal spacing of 225mm. Thus the total storage capacity is 480 assemblies (57.6 tHM).

Phase 2 comprises three storage bays in a row, a loading bay, a decontamination well for the cask and a covered deck under which the cask transporter vehicle is located. The storage capacity of phase 2 is somewhat different, each bay accommodates four fuel racks with a capacity of 130 assemblies (total for all pools is 187.2 tHM).

Germany

A wet storage facility, similar to the Bulgarian store is in operation at the Greifswald site. A decision to defuel the units and move all fuel to dry store was made after all units were mothballed. A dry cask storage facility using CASTOR casks was selected. The store has been licensed and presently is being commissioned.

Hungary

The pool storage capacity at Paks Power Station was expanded almost twofold by reracking, during 1984–1987, after the first units were commissioned.

During the years 1991 and 1992 following an evaluation of the different spent fuel storage systems, the GEC ALSTHOM ESL Modular Vault Dry Store System has been selected in order to ensure the continuous operation of the Paks NPP. The operation of Phase 1 (three vaults) has started in late 1997. Loading of fuel in the vaults of the second phase (four vaults) is expected to start early 2000. A decision to continue with the construction of Phase 3 (four further vaults) was made in 1999.

The transfer cask reception building is a separate facility adjacent to the first vault module. It houses the equipment necessary to handle and position the transfer cask prior to fuel assembly removal/drying operations. The transfer cask reception building also houses service and plant rooms, ventilation

systems and provides health physics facilities for operating staff and monitoring equipment.

The MVDS provides for the vertical dry storage of irradiated fuel assemblies in a concrete vault module. The principal components are a concrete and structural steel vault module housing an array of steel fuel storage tubes each with a removable steel shield plug. Each fuel storage tube houses a single fuel assembly. Nitrogen is used in the tubes to provide an inert atmosphere. The reinforced concrete structure of the vault is covered by a structural steel building to form a charge hall.

A fuel handling machine moves the fuel assembly from a water-filled transfer cask (C-30) to the fuel storage tube via a drying tube. The fuel handling machine operates in an enclosed volume above the fuel storage tubes referred to as the charge hall.

Kazakhstan

The single fast breeder operating in the country was shut down in May 1999. Fuel has been moved by NAC to dry storage casks in a U.S.-supported project.

Lithuania

The country has a single nuclear power plant (Ignalina) with two RBMK-1500 reactors.

Spent fuel assemblies discharged from the reactor are cooled in the AR pool for at least one year. At this point, they may be removed from the pool for cutting in the hot cell of the reactor building. The assemblies are cut into halves (two fuel bundles with the central rods and carrier tubes removed) and placed into 102-seat transport baskets and moved to the AR spent fuel pools for storage.

An interim spent fuel storage facility which uses CASTOR dual purpose storage and transport casks has been constructed. Baskets with spent fuel assemblies remain in the storage pools until they are loaded into CASTOR casks to be transferred to the dry storage facility site. Failed fuel assemblies will not be stored in the dry storage facility.

The facility is planned to be constructed in several stages: the first stage has a capacity of 72 casks. Subsequent stages will be constructed as needed. Licensing of a new dry concrete cask system (CONSTOR) is underway for the subsequent stages.

The storage site is surrounded by a reinforced concrete shielding wall and a security fence. Casks are stored in a vertical orientation on a reinforced concrete pad.

Romania

Romania operates a single CANDU unit, the second is under construction with three more units planned. The AR fuel bay of the reactor provides 10 years of interim storage at the design discharge rate. A dry concrete storage system is under investigation.

Russia

In addition to the AR pools, Russia is operating wet AFR storage facilities for RBMK fuel at Kursk, Leningrad and Smolensk. Other wet AFR storage facilities for WWER fuel are operating at the Novo-Voronezh NPP, the Mayak reprocessing plant in Chelyabinsk, and at the RT-2 reprocessing plant to be built in Krasnoyarsk. This second reprocessing plant for WWER-1000 fuel was planned, but the project was postponed, and may be cancelled completely. The RBMK storage facilities have generally increased already their storage capacity by modifying the construction of fuel hangers and moving the assemblies nearer to each other.

AFR facility at Novo-Voronezh NPP

The AFR (RS) WWER-1000 facility is located at the Novo-Voronezh NPP site. The design capacity is 400 tHM. Fuel assemblies are stored in racks at a space of 400 mm in a triangular arrangement under water shielding.

The storage bays are located in a row on either side of the cask reception room. The decontamination area accommodates a facility for cask decontamination and painting. The cask reception room has a stepwise configuration with two locations. In the upper location the cask lid is removed and in the lower location the cask is unloaded. The storage bays communicate with each other through openings with gates. The storage bays are rectangular ferro-concrete structures with dimensions of $6{,}200 \times 4{,}400 \times 16{,}400$ mm with double lining and leakage collection from behind the liner.

The AFR (OS) storage facility at Mayak

The interim AFR(OS) wet storage facility is located at the site of the Mayak Reprocessing Plant in Chelyabinsk. This facility reprocesses WWER-440 and research reactor (submarine) fuel.

The facility comprises a reception, storage, and process engineering areas. Fuel is stored in baskets. Its capacity is 560 tHM.

Krasnoyarsk AFR (OS) storage facility

The storage facility is located at the RT-2 reprocessing plant site in Krasnoyarsk. The facility was designed to hold up to 6,000 tHM of spent WWER-1000 nuclear fuel in baskets in readiness for fuel reprocessing in the RT-2 reprocessing plant.

The storage pool consists of 15 bays, with one reserve bay. The bays are connected to one another and to the unloading pool via a transport corridor. Baskets with fuel assemblies are placed on the pool floor. The pool is a rectangular shaped structure measuring $11{,}300 \times 3{,}450 \times 8{,}400$ mm and lined with stainless steel. It is separated from the transport hall by a metal deck with slots, which are closed with flap covers. The slot openings afford a fixed pitch for the rows of baskets since the basket is carried on a rod by a 16-t crane along the open slot in the deck. The fixed pitch prevents the possible collision of baskets. The pool can accommodate between 69 and 84 baskets, however, capacity can be increased if the central transport channel is also filled up.

An agreement has been signed with SGN to build two dry vault stores of the CASCAD design. The agreement allows for the construction of a 5,000 tHM capacity store at Smolensk Nuclear Power Station and another of 8,000 tHM capacity at Kursk Power Plant.

An alternative being reported is the transport of RBMK fuel also to the RT-2 site for temporary pool storage.

A ferro-concrete dual-purpose cask is in the licensing process.

Slovakia

Slovakia has a wet storage facility, similar to those mentioned at Bulgaria and Germany, at Bohunice. The facility is undergoing renovation. As a part of the renovation, the capacity of the facility will be increased (from 600 to 1,400 tHM) by using new higher capacity baskets and providing more dense filling of the pools.

The facility consists of three working bays and one reserve bay all interconnected by a water channel. The structure including all the service areas occupies a space of about 45 m × 66 m. The pools are located at ground level and there is a substantial sized reception bay for transport containers. An overhead crane of 125/20-t capacity lifts the casks into an unloading well and the fuel is removed by a 15-t bridge crane into an assembly washing area before transferring to the storage bays.

Slovenia

Slovenia's single nuclear power plant unit has its pool reracked. A second reracking serving for the whole, expected lifetime of the plant is planned.

Ukraine

Ukraine currently has one AFR wet storage facility for their RBMK fuel in Chernobyl. The design and storage technology of this facility is the standard for AFRs used for storing spent fuel from RMBK-1000 reactors.

A VSC storage facility is under construction at Zaporozhe, but licensing is delayed.

An AFR facility will be constructed at the Chernobyl site, according to a contract signed by the European Bank for Reconstruction and Development's (EBRD) Nuclear Safety Account and a consortium of French companies led by FRAMATOME. The new facility, based on NUHOMS canister technology licensed to FRAMATOME, will be designed to store 25,000 assemblies for 100 years.

All other Ukrainian NPPs are in the process of investigating the possibility to construct an AFR facility on their site.

CALENDAR

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; Website, 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; Website, 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 9-11
Plutonium 2000—International Conference on the Future of Plutonium, SAS Radisson, Brussels, Belgium. Sponsor: European Nuclear Society, the American Nuclear Society, the Russian Nuclear Society, and the Atomic Energy Society of Japan. Contact: Vincent Schryvers, BNS, Ravenstein Street, 3—1000 Brussels, Belgium; E-mail, Pu200@belgonucleaire-be

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, 847/480-9573; fax, 847/480-9282; E-mail, inmm@inmm.org; Website, http://www.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; phone, 905/823-9060, Ext. 3232; E-mail, moang@aecl.ca.

September 3-7, 2001
PATRAM 2001, Chicago, Ill., U.S.A. Sponsors: U.S. 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, 847/480-6342.

ADVERTISER INDEX