India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Security

ISBN
978-0-309-28976-4

186 pages
6 x 9
PAPERBACK (2013)

Rita Guenther, Micah Lowenthal, Rajaram Nagappa, and Nabeel Mancheri, Rapporteurs; Committee on India-United States Cooperation on Global Security: Technical Aspects of Civilian Nuclear Materials Security; National Academy of Sciences; National Institute for Advanced Studies, Bangalore, India

India–United States Cooperation on Global Security

Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security

Rita Guenther, Micah Lowenthal,
Rajaram Nagappa, and Nabeel Mancheri
Rapporteurs

Committee on India-United States Cooperation on Global Security:
Technical Aspects of Civilian Nuclear Materials Security

NATIONAL ACADEMY OF SCIENCES
THE NATIONAL ACADEMIES

In Cooperation with the National Institute for Advanced Studies, Bangalore, India

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This project was supported by Contract/Grant No. 4000112326 UT-Battelle, LLC. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number 13: 978-0-309-28976-4
International Standard Book Number 10: 0-3069-28976-9

Limited copies of this report are available from the Committee on International Security and Arms Control, 500 5th Street, N.W., Washington, DC 20001, (202) 334-2811, cisac@nas.edu.

Additional copies of this report are available for sale from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. C. D. Mote, Jr., is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. C. D. Mote, Jr., are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON INDIA-UNITED STATES COOPERATION ON TECHNICAL ASPECTS OF CIVILIAN NUCLEAR MATERIALS SECURITY: A WORKSHOP

Raymond Jeanloz, *Chair*, University of California, Berkeley
Stephen P. Cohen, Brookings Institution, Washington, D.C.
Cherry Murray, Harvard University, Cambridge, MA
William H. Press, University of Texas, Austin

National Research Council Staff

Rita S. Guenther, Study Director
Micah D. Lowenthal, Director, Committee on International Security and Arms Control
Heather Chiarello, Senior Program Assistant
La'Faye Lewis-Oliver, Administrative Coordinator

Preface and Acknowledgments

The U.S. government has made safeguarding of weapons-grade plutonium and highly enriched uranium an international policy priority and convened the 2010 Nuclear Security Summit in Washington, D.C., on April 12 and 13, 2010. Forty-six governments sent delegations to the summit and twenty nine of them made national commitments to support nuclear security. During the Summit, India announced its commitment to establish a Global Centre for Nuclear Energy Partnership, which includes a school on nuclear material security among its five major components. The Centre is to be open to international participation through academic exchanges, training, and research and development efforts.

The Centre is "aimed at strengthening India's cooperation with the international community in the areas of advanced nuclear energy systems, nuclear security, radiological safety and radiation technology applications in areas such as health, food and industry".[1] In November 2010, the United States and India signed a memorandum of understanding that provides a general framework for cooperative activities under India's Centre. According to the White House, "In working with India's Centre, the United States intends to give priority to discussion of best practices on the security of nuclear material and facilities, development of international nuclear security training curricula and programs, conduct outreach with nuclear industry, and cooperation on other nuclear security activities as mutually determined".[2]

As India builds its Centre, and as the United States endeavors to fulfill its commitment to assist in the development of the Centre, the U.S. National Academy of Sciences (NAS), together with its partner of more than 15 years, the National Institute for Advanced Studies (NIAS) in Bangalore, India, held a joint Indian-U.S. workshop to identify and examine potential areas for substantive scientific

[1]Government of India. Ministry of Science and Technology. 13 August 2010. "Global Centre for Nuclear Energy Partnership." Available at: http://pib.nic.in/newsite/erelease.aspx?relid=64718. Accessed September 20, 2013.

[2]U.S. Government. The White House Office of the Press Secretary. 8 November 2010. "Fact Sheet on U.S.-India Nuclear Security Partnership." Available at: http://www.whitehouse.gov/sites/default/files/india-factsheets/Fact_Sheet_on_Nuclear_Security.pdf. Accessed September 20, 2013.

and technical cooperation between the two countries on issues related to nuclear material security. Because of decades-long legal restrictions regarding U.S. cooperation with India on nuclear technology, the Indian and U.S. nuclear energy and technology enterprises developed independently. The aim of this workshop was to convene technical experts from India and the United States, to begin discussions about nuclear material security, and to identify promising opportunities for India and the United States to learn from each other and cooperate.

In preparation for the workshop, NAS formed a planning committee, headed by Raymond Jeanloz, comprised of prominent scientists, engineers, and a South Asia expert. The planning committee members and NAS staff worked collaboratively with nuclear material security experts, NIAS leadership, and faculty to develop the agenda for the workshop. The National Institute of Advanced Studies (NIAS) is a premier research institute in India, founded in 1988 and located in Bangalore. NIAS is engaged in multi-disciplinary research and is unique in its integrated approach to the study of the intersections between science and technology, social issues, humanities and leadership. The International Strategic and Security Studies Program (ISSSP) at NIAS has been active since 1996. Research conducted by faculty and students of the Program emphases science and technology issues and their integration with policy as well as organizational and institutional arrangements. ISSSP is a Track-II dialogue partner with the Committee on International Security and Arms Control (CISAC) of the U.S. National Academy of Sciences. Over more than 15 years, the series of dialogue meetings has contributed to a better understanding of bilateral strategic issues.

During a planning trip taken by NAS planning committee members and staff in June 2012, the two groups met and refined the agenda, identified potential speakers, and determined other elements of the workshop. In addition, during the planning trip, the NAS delegation met with key officials in the Government of India who provided their support for and input to the workshop.

Following the planning trip, the two groups finalized the agenda for the joint workshop, held on the NIAS campus October 29-31, 2012, which included a variety of technical issues in nuclear materials management, such as nuclear materials accounting, cybersecurity, physical security, and nuclear forensics. The workshop enabled Indian and U.S. experts to describe their work and plans for future activities on each topic.

The following summary intentionally includes a large portion of the material discussed during the workshop to provide readers with extensive insights into the views of the Indian and U.S. participants. An overarching theme which emerged from this detailed discussion was the difference of views faced in India between the need to develop greater energy capacity to expand economic growth and development for the country's population overall, and at times strong opposition to nuclear power by Indians concerned about the safety and security of the facilities. This tension was also experienced in the United States when nuclear power grew there in previous decades. A second theme that emerged was the different development paths taken by India and the United States as their nuclear programs grew, largely in isolation from one another. As a result, the technical approaches detailed

here will be of interest to many readers. For those readers interested in a higher level overview of the workshop discussions, key messages and promising topics for collaboration arising from the presentations and discussions have been added at the beginning of each topical chapter.

The U.S. National Nuclear Security Administration (NNSA) funded NAS to conduct this workshop. Oak Ridge National Laboratory handled the contract for NNSA. In addition, the U.S. Department of State, Sandia National Laboratory, and the Patel Endowment at the NAS funded the travel costs for several U.S. participants. NIAS provided substantial financial support for the workshop by providing housing and meals for participants as well as providing the facilities and administrative and technical support for the workshop. The generous support of all sponsors is greatly appreciated.

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Academies' Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for quality and objectivity. The review comments and draft manuscript remain confidential to protect the integrity of the process.

We wish to thank the following individuals for their review of this report: Ian Hutcheon, Lawrence Livermore National Laboratory; L.V. Krishnan, National Institute for Advanced Studies; George Perkovich, Carnegie Endowment for International Peace; and Shri A.R. Sundararajan, Safety Research Institute.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the content of the report, nor did they see the final draft before its release. Responsibility for the final content of this report rests entirely with the rapporteur(s) and the institution.

Technical experts of both India and the United States, as demonstrated during this workshop, seek opportunities to work together on issues related to nuclear materials security. While the task of securing these materials is vast, so too is the experience and expertise available in our two countries to meet this challenge. Joint efforts such as this workshop provide the basis for India and the United States to continue to learn from each other, to exchange ideas for collaborative efforts, and to increase the confidence and support necessary to take their cooperation farther as they secure civilian nuclear materials in their respective countries.

Contents

Synopsis

For more than two decades, beginning first with the breakup of the Soviet Union in 1991, followed by the terrorist attacks of September 11, 2001 in the United States, and the terrorist attacks in Mumbai on November 26, 2008, increasing attention has been paid to the security of nuclear materials around the world. A growing number of nations recognized a need for higher levels of security for civilian nuclear materials, such as uranium ore concentrate, low-enriched and especially highly enriched uranium, uranium fuel, plutonium used in power or research reactors, spent fuel from reactors, and other materials that can fission. The workshop summarized in the following chapters focused on all types of civilian nuclear materials (those that emit radiation but do not fission), with the exception of radiological materials, choosing to emphasize those nuclear materials that are frequently used in power facilities, research facilities, reprocessing facilities, and other facilities associated with nuclear power generation and/or research activities.

With the aim of enhancing the security of these nuclear materials, the National Academy of Sciences (NAS), together with the National Institute for Advanced Studies in Bangalore (NIAS), organized and convened a workshop entitled, "India-United States Cooperation on Global Security: A Workshop on Technical Aspects of Civilian Nuclear Materials Security," held October 29-31, 2012 in Bangalore, India, on the NIAS campus. The goal for the workshop is described succinctly in the statement of task in Box S-1.

GOALS AND OBJECTIVES FOR JOINT WORKSHOP

The workshop consisted of sessions on the following topics: an overview of civilian nuclear materials; a systems approach to security; physical security at civilian nuclear facilities; cybersecurity at civilian nuclear facilities; the importance of people in security of civilian nuclear facilities; nuclear forensics; nuclear energy and the challenge of development in India; and a systems approach to security at civilian nuclear facilities. Each of these sessions is described in a chapter of the

summary bearing the same name. To focus these sessions and discussions, NAS and NIAS developed the following goals and objectives for the joint workshop:

- To build mutual understanding of how experts in India and the United States approach issues of civilian nuclear materials management and security;
- To establish contacts among Indian and U.S. scientists and experts on nuclear materials security and to enhance confidence in cooperation on nuclear security issues; and
- To identify concrete, technically-based areas for potential future collaboration between the technical experts of India and the United States, including through the Global Centre for Nuclear Energy Partnership.

BOX S.1: STATEMENT OF TASK

The U.S. National Academy of Sciences working with the Indian National Institute for Advanced Studies will convene a joint workshop to identify and examine potential areas for scientific and technical cooperation between the United States and India on issues related to nuclear material security. The workshop may identify options for work that is of mutual interest for technical collaboration under the newly signed Memorandum of Understanding for the Indian Global Centre for Nuclear Energy Partnership. The agenda for the workshop will be developed jointly with Indian counterparts, but could include a variety of technical issues in nuclear materials management, such as nuclear materials safeguards, detection, monitoring, and nuclear forensics. The National Academy of Sciences will provide an individually-authored summary of the workshop.

KEY ISSUES FROM WORKSHOP

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

Introduction and Overview of Civilian Nuclear Materials

- Civilian nuclear material is found in many countries around the world, although exact quantities are not known.
- Even countries that do not have fissile materials may be used as transit countries for illicit transport of nuclear materials.

- Finding a balance between public concerns about nuclear energy and the need for greater electrical capacity is extremely difficult at present. These challenges increased sharply immediately after the situation with the Fukushima Daiichi nuclear plant following the tsunami on March 11, 2011.
- Planning for the expansion of nuclear power in India as a part of the larger energy picture to support economic growth more broadly in the context of a growing population, much of which is rural, is very challenging.
- In the long term, India is working to develop proliferation-resistant fuel cycles.
- Public acceptance of the use of nuclear materials for nuclear power is based on experts' assurances that nuclear materials will remain under control and appropriate use, and that the public will not be harmed either by a safety incident or a security incident.
- Using technologies and techniques for material control and accounting to balance and complement nuclear security is how operators maintain as much control over the nuclear material as possible, while still being able to use it for its intended purposes.

Systems Approach to Security at Civilian Nuclear Facilities

- Weapons-usable material must be kept out of the hands of adversaries who may be trying to get their hands on this material and could use it for malevolent actions.
- No material is absolutely safe, and any material is vulnerable at some level.
- Nuclear security is a continuous, dynamic risk management job and requires constant and vigorous efforts.
- Program resources are to be used for both safety and security. The balance of risk and security as well as the balance of resources needs to be maintained to not undermine employees' interest in maintaining high quality science as well as vigilance of safety and security measures.
- In India, the primary security concern at civilian nuclear facilities is sabotage.
- Several safety features can be incorporated into reactors, which also aid security.
- Material categorization is also essential to the security design process because there is a direct relationship between the protection required and the quantity of the material and its enrichment level.
- Apart from resource extension, the closed fuel cycle can be designed to be more proliferation resistant.

Physical Security at Civilian Nuclear Facilities

- Nuclear security has three distinct steps: (1) define the requirements, (2) design the physical protection system based on the requirements, and (3) evaluate the physical protection system to assess whether it meets the performance requirements.
- The most difficult adversaries to address using the physical protection system are terrorists, but activists and demonstrators are also difficult because of the ambiguity of their actions and intentions.
- The insider threat is a worldwide concern for nuclear security because an adversary with a colluding insider is very dangerous.
- The vulnerability assessment process can be divided into three broad phases: characterization (target identification); analysis (identifying vulnerabilities); and neutralization and system effectiveness.

Cybersecurity at Civilian Nuclear Facilities

- Cybersecurity refers to the prevention, detection, and mitigation of unauthorized attempts to control or disable computers and electronic control systems as well as protection of information in computer databases.
- Cybersecurity for a nuclear facility can be divided into two parts: instrument and control security, and facility network security. There are several differences between these parts of security, including different methodologies, mechanisms, and the effect of failure in each domain.
- Cybersecurity is commonly understood to have three attributes: confidentiality, availability, and integrity.
- Security risks cannot be reduced to zero. Managing instrument and control security requires a systematic, comprehensive, and dynamic methodology.
- Every day new viruses, new vulnerabilities, and new problems are found with the systems.

The Importance of People in Securing Civilian Nuclear Facilities

- Every person, from a custodian to a technician to a scientist to a guard in the protective force, needs to believe in and support the nuclear security program for it to succeed. This is nuclear security culture.
- The driving motivations for the Indian Global Centre for Nuclear Energy Partnership (GCNEP) are first global cooperation and second the technical issues of safety, security, and proliferation resistant design as the three pillars on which the Centre will stand.
- Specifically, the GCNEP School for Radiological Safety Studies is designed to contribute significantly to nuclear security, particularly in the area of radiation sources.

- Unless we update ourselves, unless the security forces, the response forces, the guard forces, and the security operators update themselves with the current threat scenarios, with current practices, with current systems and techniques used, and also with regulatory procedures or by other requirements, it will not be possible to maintain proper and effective nuclear security.

The Emerging Science of Nuclear Forensics

- There are strong scientific capabilities in nuclear forensic science but our ability to interpret these data is still in a state of development.
- Expanded databases with information on nuclear material around the world are needed.
- Greater understanding of how materials change as they undergo reprocessing and other processes is needed.
- No single technique provides the needed information for all or even any material.
- Nonproliferation nuclear forensics requires a focused international cooperative effort.

Implementing Systems Approaches to Security at Civilian Nuclear Facilities

- Security is a national responsibility but has international dimensions.
- Communication with the public is important because in an accident or disaster scenario, there is not time to really explain thoroughly.
- Decision making in an unexpected emergency scenario would involve multiple players: political leaders, operators, regulators, bureacrats, politicians, representatives of the local community, and others.
- The balance between research and security interests is at times difficult to define and maintain.

Nuclear Energy and the Challenge of Development in India

- India faces many acute challenges of energy development, which has caused the country's leaders to consider India's indigenous energy sources and how it can increase energy supply to better meet the exponentially expanding energy demand.
- Given this demand, India has chosen to pursue nuclear energy as a source of energy, and is planning a rapid expansion of the nuclear power sector in the coming decades.
- Green scenarios (solar, nuclear, or a combination) should be considered.

- Development deficits and lack of sufficient energy are also issues that could create their own security problems over time.
- India has chosen to develop a closed fuel cycle because of its limited domestic sources of uranium.

BUILDING ON THE SUCCESS OF THE WORKSHOP

Technical experts in a variety of fields associated with civilian nuclear materials security provided presentations and engaged in frank discussions. These experts were chosen by the workshop organizers from the national laboratories, academia, and non-governmental organizations of their respective countries. Over the course of the three-day workshop they provided their perspectives, knowledge and experience and shared ideas for possible future joint collaborations in this area between India and the United States. The concluding session of the workshop identified initial areas of possible cooperation that emerged through the presentations and discussions.

1

Introduction and Overview of Civilian Nuclear Materials

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- Civilian nuclear material is found in many countries around the world, although exact quantities are not known.
- Even countries that do not have fissile materials may be used as transit countries for illicit transport of nuclear materials.
- Finding a balance between public concerns about nuclear energy and the need for greater electrical capacity is extremely difficult at present. These challenges increased sharply after the situation with the Fukushima Daiichi nuclear plant following the tsunami on March 11, 2011.
- Planning for the expansion of nuclear power in India as a part of the larger energy picture to support economic growth more broadly in the context of a growing population, much of which is rural, is very challenging.
- In the long term, India is working to develop proliferation-resistant fuel cycles.
- Public acceptance of the use of nuclear materials for nuclear power is based on experts' assurances that nuclear materials will remain under control and appropriate use, and that the public will not be harmed either by a safety incident or a security incident.
- Using technologies and techniques for material control and accounting to balance and complement nuclear security is how operators maintain

as much control over the nuclear material as possible, while still being able to use it for its intended purposes.

Promising Topics for Collaboration Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions are not those representing the consensus of the participants, but are rather a selection of those topics offered by individual participants throughout the presentations and discussions.

- There is a high degree of uncertainty about accounting for materials in nuclear waste. Despite efforts to reduce the amount of plutonium or uranium that goes into waste, one cannot eliminate it entirely. This is an area in which cooperation has a great deal of potential.
- Measurement control, including questions such as how uncertainties combine, and which measurement methods are particularly problematic, are areas for joint collaboration.
- Indian and U.S. experts could work on nondestructive analysis to develop additional ways or techniques to help further establish how measurement standards are defined and characterized and the pedigree of material or accuracy of measurements.

The U.S. government has made safeguarding weapons-grade plutonium and highly enriched uranium an international policy priority, and convened The 2010 Nuclear Security Summit in Washington, D.C., on April 12 and 13, 2010. Forty-six governments sent delegations to the summit and twenty-nine of them made national commitments to support nuclear security. During the Summit, India announced its commitment to establish a Global Centre for Nuclear Energy Partnership. The Centre is to be open to international participation through academic exchanges, training, and research and development efforts.

The Centre is "aimed at strengthening India's cooperation with the international community in the areas of advanced nuclear energy systems, nuclear security, radiological safety and radiation technology applications in areas such as health, food and industry".[1] In November 2010, the United States and India signed a memorandum of understanding that provides a general framework for cooperative activities in working with India's Centre. According to the White House, "In working with India's Centre, the United States intends to give priority to discussion of best practices on the security of nuclear material and facilities, develop-

[1]Government of India. Ministry of Science and Technology. 13 August 2010. "Global Centre for Nuclear Energy Partnership." Available at: http://pib.nic.in/newsite/erelease.aspx?relid=64718. Accessed September 20, 2013.

ment of international nuclear security training curricula and programs, conduct outreach with nuclear industry, and cooperation on other nuclear security activities as mutually determined".[2]

As India builds its Centre, and as the United States endeavors to fulfill its commitment to assist in the development of the Centre, the U.S. National Academy of Sciences (NAS), together with its partner of 15 years, the National Institute for Advanced Studies (NIAS) in Bangalore, India, organized a joint Indian-U.S. workshop entitled, "India-U.S. Cooperation on Global Security: A Workshop on Technical Aspects of Civilian Nuclear Materials Security," held October 29-31, 2012 on the NIAS campus in Bangalore, India. The aims of the workshop were to identify and examine potential areas for substantive scientific and technical cooperation between the two countries on issues related to nuclear material security, to establish scientist-to-scientist contacts between experts in nuclear materials management in the United States and counterparts in India, and to build confidence in cooperation on nuclear security issues. The hope is that if the technical community identifies concrete, technically-based areas for potential future collaboration, these could be the foundation for progress at the Centre and between the two countries more broadly.

Workshop participants, technical experts in a variety of fields associated with civilian nuclear materials security, provided presentations and engaged in frank discussions. These experts were chosen by the workshop organizers from their countries' national laboratories, academia, and non-governmental organizations. Over the course of the three-day workshop they provided their knowledge and experience and shared ideas for possible future joint collaborations in this area between India and the United States. The concluding session of the workshop identified initial areas of possible cooperation that had emerged through the presentations and discussions. This report provides a factual summary of the workshop presentations and discussions. There was no attempt to reach consensus findings and recommendations.

CIVILIAN NUCLEAR MATERIALS: OVERVIEW

R. Rajaraman provided workshop participants with an overview and introduction to nuclear materials. He began by stating that until recently, "nuclear materials" were frequently understood to be synonymous with the term "fissile materials." Fissile materials are directly weapon-usable, and therefore considered the most dangerous. Today, however, he explained, "nuclear materials" are often defined more broadly and include radiological materials: "just plain natural uranium ore, industrial uranium or depleted uranium, plutonium isotopes

[2]U.S. Government. The White House Office of the Press Secretary. 8 November 2010. "Fact Sheet on U.S.-India Nuclear Security Partnership." Available at: http://www.whitehouse.gov/sites/default/files/india-factsheets/Fact_Sheet_on_Nuclear_Security.pdf. Accessed September 20, 2013.

produced in reactors, spent fuel from reactors, all radioactive substances, fissile or not." Fissile materials, the nuclear materials of focus in this workshop, are those that undergo nuclear fission easily without adding energy. Specifically, these materials are uranium-235, uranium-233, and different isotopes of plutonium. Other materials, such as americium and neptunium, are technically fissile, but are not typically used in significant quantities in the civilian nuclear power cycle.

Rajaraman explained that natural uranium contains less than 1 percent of uranium 235. "The bulk of natural uranium, such as uranium-238, cannot sustain fission. But even that tiny fraction of less than 1 percent is sufficient to fuel heavy water-moderated reactors, like our reactors in India." Plutonium is not found in nature. It is a by-product of nuclear reactions in the fuel rods of nuclear reactors. In India, plutonium is separated from the fuel rods in reprocessing units. There is not sufficient fissile material in spent fuel to sustain a fission chain reaction unless the plutonium is separated and concentrated in new fuel.

Civilian nuclear material is found in many countries around the world, although exact quantities are not known. According to the Fissile Materials Group, Russia and the United States have the largest quantities of nuclear materials in the world. It is estimated that in total there are about 1400 tons of highly-enriched uranium (HEU) in the world and about 495 tons of separated plutonium.[3] The current worldwide stocks of fissile material together can fuel 170,000 nuclear warheads. While much of this material exists in the military sector, a significant quantity is in the civilian sector which underscores the importance of continuously securing this material.[4]

Rajaraman presented the distribution of civilian HEU around the world. The non-nuclear weapons states (as defined by the Treaty on the Non-Proliferation of Nuclear Weapons [NPT]) have about 10 tons of HEU, or sufficient fuel for approximately 400 warheads. Rajaraman noted that even countries that do not have fissile material may be used as transit countries for illicit transport of nuclear material. Therefore, he noted, responsibility for securing fissile materials cannot be limited to countries with nuclear weapons, but rather it must be a truly cooperative international effort.

Rajaraman believes that the nuclear summits are an example of international cooperation on nuclear materials security. From an Indian perspective, one of the reasons for the success of the nuclear security summits—the initial summit in Washington and the second summit in Seoul, Korea in 2011—was that the highest level of Indian leadership was invited to participate, setting them on equal footing with nuclear weapons states. During the Washington summit, India, Japan, China, and Italy announced the creation of new centers of nuclear security technologies and training. The summit process, and the commitments of participating countries,

[3]See Global Fissile Material Report, 2011. Available at http://fissilematerials.org/library/gfmr11.pdf (p3)

[4]*Ibid*, p. 11 and p. 29.

emphasize that nuclear terrorism continues to be one of the most challenging threats to international security.

BALANCING ENERGY NEEDS AND NUCLEAR MATERIALS SECURITY

Public Concerns about Nuclear Energy and Development Efforts

M. R. Srinivasan, former chairman, Atomic Energy Commission (AEC) of India, provided remarks that outlined the current challenges faced by those in India who are attempting to provide increased electrical capacity for the development of the country. As he explained, finding a balance between public concerns about nuclear energy and the need for greater electrical capacity is extremely difficult at present. These challenges increased sharply immediately after the situation with the Fukushima Daiichi nuclear plant following the tsunami on March 11, 2011. In response to these events in Japan, the local population living near the Kudankulam nuclear power plant in the southern Indian state of Tamil Nadu protested by the thousands to prevent the loading of reactor fuel. These protests continued for months and involved the local villagers and those involved in fishing who protested from the water. While the protests reached their height toward the middle of 2012, opposition continues.

Srinivasan explained that he was responsible for speaking at a large number of public meetings (40-50) in many parts of India, participating in many discussion groups and television and newspaper interviews, to try to bring some kind of balance to the debate. Local politics also played a role in the local response to the nuclear plant as two leading regional political parties reversed majority and minority positions in elections. The new government attempted to meet with the public to understand their concerns and to attempt to explain the scientific and technical evidence behind the safety and security of the plant. The government established a 15 member committee, which was headed by a well-known space scientist who later studied oceanography and became an expert on tsunamis and earthquakes. That committee listened to all of the protesters' concerns, and the protesters had their own scientific advisors that raised several questions, all of which were answered by the committee.

The opposition was led by a group called the People's Movement Against Nuclear Energy. Srinivasan stated that unfortunately they were not concerned with the safety of the Kudankulam plant. Rather, their objective was to have no nuclear energy at all. So they just sat across the table and listened to voluminous explanations about the plant's safety features and said, "no we don't want to look into all of these things. We don't want this power plant to be started. It is as simple as that."

Srinivasan was then asked by the Chief Minister of Tamil Nadu to chair another committee to review the work of the first committee established by the Government of India. The goal was again to examine the concerns of the people and talk to them and find a resolution to the stalemate. Srinivasan and his

colleagues also went through the safety features and focused on those related to the geological, seismological, and tusunami-related issues, which were the greatest concerns of the people. There were no scientific or technical reasons to stop the project because the safety issues were addressed by an advanced, third-generation-plus reactor design, and by the fact that the site does not have seismic or tsunami activity as had Fukushima. The committee also explained that there was an additional special feature of the Kudankulam reactor, the passive safety system, incorporated into the design to ensure that the reactor fuel would continue to be cooled even in the event of a loss of power to the reactor. At the request of the Indian safety authorities, this special design feature was incorporated to dissipate the residual heat to air through a set of very large radiators, located outside the reactor building. Again, a protestor said, "no, we are not interested in all of these explanations," Srinivasan said. Regardless of these objections, the first fuel was loaded into the reactor vessel and power generation was to begin in December 2012.

This situation not only illustrates the difficulties in communicating safety issues surrounding nuclear power, it also illustrates real security concerns. Srinivasan stated that during the protest, a population of about one or two thousand protestors virtually held seige to the plant. They blockaded entry to the power plant and personnel could not enter. They said, "no, we don't want these large workforces to come in because we want this work to be suspended." They only wanted to let about 20 or 30 people in to maintain the essential services such as water purity, temperature control, and the like. As work resumed, Srinivasan advised the deployment of significant security forces to ensure safety and security. On one occasion, approximately 400 fishing boats approached by water and people attempted to enter the plant's premises.[5]

He noted that a lot has been learned, but there is still a lot more that can be learned regarding how to address such situations. These lessons may be relevant to other situations as well because India is experiencing a great deal of opposition to many projects, including mining projects, hydraulic projects, coal-fired power station projects, nuclear projects, steel plants, and others. This presents a significant challenge as the energy needs of the country that reached a new peak in the last 18 months due to a combination of factors.

The last monsoon brought less rain causing hydroelectric stations to reduce the amount of power they could generate. Coal stocks at 47 coal-fired power stations are at a critically low level, reducing power generation by 65,000 megawatts of generation capacity. Gas-fired plants are also reducing capacity due to a lack of Indian gas supplies. The predicted increase in capacity of gas supplies

[5]Fishermen lay siege to Kudankulam nuclear plant, Rediff.com News, 08 October 2012. Available at http://www.rediff.com/news/slide-show/slide-show-1-fishermen-lay-siege-to-kudankulam-nuclear-plant/20121008.htm#1.

by 50 percent from off-shore fields in the eastern part of India did not occur. [6] In combination, the lack of hydroelectric power as well as coal and gas electrical sources has reached a critical point. At the same time, protests continue against these power-generation sources and the news media reports on the protests. Srinivasan noted that few people in industry, business, or academia enter this debate and the media does not receive balanced information. This situation presents a challenge because to sustain economic growth rates of eight or nine percent, more energy is needed. This raises a sociological issue as well challenges associated with the distribution of gains from development.

Since the debates between 2005 and 2008 about the ability of India to purchase uranium on the international market, in which Srinivasan participated as a member of the AEC, he notes that India has been able to purchase natrual uranium and low-enriched uranium from Russia, Kazakhstan, and other countries. This has allowed Indian reactors to run at about 80 percent capacity or higher. That said, although the Indian nuclear power program dates back to the 1950s, it only generates 5,000 megawatts of nuclear electricity from 20 reactors, not including the two large reactors of Russian design in Kudankulam. Of these 20, 16 were designed and built in India. India also has small reactors, mostly 220 megawatts and two of them are 540 megawatts, and work has begun on a number of 700-megawatt units of domestic design, four of which are under construction and a total of at least 12 are anticipated.[7]

Srinivasan concluded by reiterating that India is interested in developing its nuclear industry and producing significantly greater quantities of nuclear-generated electricity, and to do this, India will need to cooperate with international partners, in addition to addressing continuing domestic concerns of safety and security.

Planning for Nuclear Energy Expansion while Maintaining Security

Ravi Grover noted the challenges of planning for the expansion of nuclear power to support economic growth and an increasing population, much of which is rural. He began by stating that India has seen impressive economic growth for close to two decades despite several challenges, one of which is the ability of existing and expanding infrastructure to support that growth. "Energy is the most important part of that infrastructure, and it has been a major challenge for the Department of Atomic Energy (DAE) to ensure that adequate ener-

[6]The projected demand for 2011-12 was 89 BCM (Ref: Appra Zaifrani and Karthik Madhavan, The Gas Sector MBA Thesis, p. 15 available at http://www.slideshare.net/kadweiser/natural-gas-in-india). The actual production was 47.559 BCM (Ref: Government of India, Ministry of Petroleum and Natural Gas, Indian Petroleum and Natural Gas Statistics 2011-12, p. 3, available at http://petroleum.nic.in/pngstat.pdf.

[7]Nuclear Power Corporation of India website-Plants under operation. Available at http://www.npcil.nic.in/main/AllProjectOperationDisplay.aspx.

gy is available. Providing energy reliably at affordable prices will continue to be a challenge, as India is not rich in energy resources."

According to the 2011 census, India's population is 1.2 billion, and 69 percent of the population lives in rural areas.[8] In spite of impressive growth in installed electrical capacity and the fact that globally India ranks fifth in terms of total electricity generation, India's per-capita electricity consumption is well below the world average. Half of rural households have no access to electricity and most of them use biomass energy.[9]

Grover relayed that DAE studied the growth of energy demand with the objective of quantifying the share of nuclear energy needed in the electricity mix in the coming five decades in India. DAE experts looked at the fuel resource position, including the potential for renewable energy sources, projected population growth, projected economic growth, and likely improvements in energy efficiency of the economy. From this they determined estimates for scenarios of growth of electricity generation in the country for the next 50 years, taking 2002-2003, which was the first year of the tenth five-year plan, as the base year. As an indicator of economic growth, DAE used a study by Goldman Sachs, which had just been published at that time.[10] For population growth, they used various forecasts available in India and hypothesized that the population will reach 1.5 billion by the middle of the 21st century.[11] DAE's study indicated that total electricity generation in the year 2052 will be almost 8,000 terawatt hours, corresponding to annual per-capita generation of 5,300 kilowatt hours. Installed capacity in the year 2052 was estimated to be close to 1,400 gigawatts.[12]

The question is, Grover stated, "Is the per-capita generation of 5,300 kilowatt hours too high for India?" There is a school of thought that says that a tropical country like India does not require heating, and therefore energy demand in India will always be less than what it is in the West where the climate is temperate. However, when one observes what is happening in India's immediate neighborhood, a different picture emerges. The per-capita energy demand in Singapore is the same as the average of Organisation for Economic Co-operation and Development countries, and the energy demand in Malaysia and Thailand is also growing.[13] One should not expect a different scenario in India. Grover further noted that

[8]Census of India, Government of India. Available at http://censusindia.gov.in/2011-prov-results/data_files/india/Final_PPT_2011_chapter3.pdf.

[9]Central Electricity Authority Government of India. Available at http://www.cea.nic.in/reports/yearly/lgbr_report.pdf.

[10]Goldman Sachs (2003), Dreaming With BRICs: The Path to 2050, Global Economics Paper No: 99. Available at http://www.goldmansachs.com/our-thinking/archive/archive-pdfs/brics-dream.pdf.

[11]*Ibid*, p. 8-10.

[12]R. B. Grover and Subhash Chandra, "A Strategy for Growth of Electrical Energy in India," Document No.10, Department of Atomic Energy, Mumbai, August 2004.

[13]IEA (2012) Key World Energy Statistics. Available at http://www.iea.org/publications/freepublications/publication/kwes.pdf.

the Planning Commission of India, in its report on integrated energy policy, forecasted a growth rate higher than that of the DAE study.[14] To put the numbers in perspective, the total energy generation by utilities and power plants combined in the previous fiscal year, which ended on 21st March 2012, was about 1,000 terawatt hours, or about one-eighth of what Grover noted as projected by the middle of the century. He noted the projected growth as a very large, but achievable task.[15]

For supply options, one has to look at the fuel resources of India, which include coal deposits, but its oil and gas reserves are quite modest. With the ever-increasing demand for coal for thermal power plants, one can safely say that the coal supply will not last for more than a few decades. Mining and transportation also present problems for the use of coal. Renewable energy sources are also a possibility, but may be insufficient.

Grover then cited a recent report by S. P. Sukhatme, former director of Indian Institute of Technology Bombay and former chairman of the Atomic Energy Regulatory Board (AERB). Sukhatme estimated the full potential of all renewable energy sources (solar thermal, solar photovoltaic, large and small hydropower, wind power on land as well as offshore, biomass, and tidal power) at 1,229 terawatt hours annually.[16] This is a very optimistic estimate, he said, but even this is nowhere near the projected annual demand of 8,000 terawatt hours that India would need by the middle of the century.[17] Nuclear energy seems to be the only possible option. A Planning Commission-initiated report on integrated energy policy has referred to nuclear energy as the most viable means of achieving long-term energy security. It calls for pursuit of a closed fuel cycle to enable India to tap into vast thorium resources, and become truly energy independent beyond 2050.[18]

Security of nuclear materials is built into the day-to-day operations of India's nuclear program. Grover defined the open fuel cycle as one which "disposes of spent fuel without extracting plutonium." He stated, "such a disposal would result in the creation of a plutonium mine for posterity," where "the security risk is aggravated if such a disposal is designed to be retrievable." To ensure that there is no buildup of the plutonium stockpile, India is strictly observing the principle of "reprocess to reuse." In India, he noted, the reprocessing of spent fuel and fast

[14]Planning Commission (2005), Draft Report of the Expert Committee on Integrated Energy Policy. Available at http://planningcommission.nic.in/reports/genrep/intengpol.pdf.

[15]Planning Commission (2012), Power and Energy, P, 342. Available at http://planningcommission.nic.in/plans/planrel/fiveyr/11th/11_v3/11th_vol3.pdf.

[16]S. P. Sukhatme (2012) Can India's future needs of electricity be met by renewable energy sources? A revised assessment, *Current Science*, Vol. 103, No. 10, 25 November, available at http://www.currentscience.ac.in/Volumes/103/10/1153.pdf.

[17]R. B. Grover and Subhash Chandra, "A Strategy for Growth of Electrical Energy in India," Document No.10, Department of Atomic Energy, Mumbai, August 2004.

[18]Planning Commission (2005), Draft Report of the Expert Committee on Integrated Energy Policy, available at http://planningcommission.nic.in/reports/genrep/intengpol.pdf.

reactor waste are being synchronized to preclude the buildup of a plutonium stockpile. Technologies for the vitrification of high-level waste from reprocessing have been developed, and vitrified waste, after it has been packed in stainless steel containers, is being stored in a solid waste civilian storage facility.

In addition, Grover noted, India has given equal emphasis to developing a sound framework for governance of nuclear power, and the Atomic Energy Act of 1962 is the main legislation in India.[19] The Act governs radiation protection, safe disposal of radioactive waste, the operation of mines and minerals, the handling of specified substances, and the irradiation of food and the like. Other legislation related to governance of nuclear power are the Mines and Minerals Act of 1957, the Weapons of Mass Destruction Act of 2005, and the recently-enacted Civil Liability for Nuclear Damage Act.[20]

Grover clarified that while India follows a nomenclature for nuclear and dual-use items that is different from that followed by the Nuclear Suppliers Group, the end objective is the same. More recently, the Government of India issued guidelines for implementation of arrangements for cooperation concerning peaceful uses of atomic energy with other countries. The AERB, the regulatory board in India, was established in 1983 to convert the regulatory body's *de facto* independence to *de jure* independence. The Nuclear Safety Regulatory Authority Bill 2011 was introduced in the Parliament and has already been examined by the relevant parliamentary standing committee.[21] The government is working on amendments to the bill in light of recommendations from the standing committee.

In addition to national legislation, India has taken additional obligations under various international mechanisms. Of particular importance for this workshop is the Convention on the Physical Protection of Nuclear Material and its 2005 amendment, the Convention on Nuclear Safety.[22] India also participates in the nuclear security summit process. For both the Washington summit and the Seoul summit, the Indian delegation was led by the prime minister, the highest diplomatic and political position in the country. At the Seoul summit, the prime minister announced a voluntary contribution to the nuclear security efforts of the International Atomic Energy Agency (IAEA). India also hosted a Sherpas meeting in preparation for the Seoul summit. Further, at the end of November 2012, India will host a workshop in cooperation with the United Nations 1540 Commission. India has also shut down its research reactor operating on highly-

[19]The Department of Atomic Energy (DAE), The Atomic Energy Act, 1962. Available at http://dae.nic.in/?q=node/153.

[20]The Department of Atomic Energy (DAE), Atomic Energy Act, Rules and Notifications. Available at http://dae.nic.in/?q=node/60.

[21]The Department of Atomic Energy (DAE), Notification of Civil Liability for Nuclear Damage Rules 2011. Available at http://dae.nic.in/writereaddata/liab_rules.pdf.

[22]IAEA, The Convention on Nuclear Safety. Available at http://www-ns.iaea.org/conventions/nuclear-safety.asp.

enriched uranium. Overall, India is trying to pursue those technologies which help minimize the problem of security of nuclear materials.

India is not resting on its laurels, he said, but is continuously trying to work further to improve nuclear security. One significant step was announced by the prime minister at the 2010 Washington summit: the establishment of the Global Centre for Nuclear Energy Partnership. The Global Centre will become an important platform for India to interact with the world community in all aspects of peaceful uses of nuclear energy, including nuclear security, safety, and nonproliferation. Extensive facilities will be set up at this center for training nuclear security professionals.

Further, to gain international experience, DAE has invited an Operational Safety Review Team from IAEA to look at two reactors in Rajasthan. Earlier, all plans of the Nuclear Power Corporation of India Limited were peer-reviewed by the World Association of Nuclear Operators. The government has also announced that a mission from IAEA will be invited for the regulatory review, which could occur next year.

Grover stated that thus far his remarks addressed the security of nuclear materials in the short and medium term. In the longer term, he said, India is working to develop proliferation-resistant fuel cycles. This effort includes developing technologies for reprocessing so that plutonium is separated along with uranium, and developing thorium-based reactor systems. The overall objective is to use nuclear science to reduce the requirement of security of nuclear materials.

In summary, India is developing a closed fuel cycle, with technologies consistent with this approach. Reprocessing is therefore pursued to reuse recovered plutonium. Further, adequate steps, including the establishment of training facilities, are being taken to secure the future. To address the issue of security of nuclear material over the longer term, research and development of proliferation-resistant technologies has been ongoing for the past several years. Grover reiterated that one should aim to use nuclear science to reduce the requirement of security of nuclear materials and address the residual requirement using standards and procedures that have been developed for this purpose.

Nuclear Material Measurements: Protecting the Public and Increasing Confidence in Safety and Security

Peter Santi of Los Alamos National Laboratory focused his remarks on nuclear material measurements and their role in not only nuclear security, but also in nuclear safety, material control and accountability, and, to some degree, in nuclear safeguards. The primary goal of all of these efforts is how to ensure that the public is not harmed by nuclear materials. Public acceptance—or potentially, new acceptance—of the use nuclear materials for nuclear power is based on experts' assurances that nuclear materials will remain under control and appropriate use, and that the public will not be harmed either by a safety incident or a security incident. This requires the establishment of three important princi-

ples associated with managing nuclear material within a nuclear facility (three S's):

- Safety: ensuring that material does not cause harm to the public or workers through an accident or through improper configurations
- Security: preventing material from leaving an authorized area or from being used improperly
- Safeguards: ensuring that material is accounted for and under constant control in the facility

With respect to safeguards, Santi rephrased this as "I know where all my material is. I know where it is going. I know what it is being used for or where it is being stored and how it's being stored. I know it is going to be leaving the facility to go to the next place, whether it be going to a fuel fabrication facility, to the nuclear reactor to be used, or to a nuclear waste facility that is an appropriate repository."

While these three principles or objectives have different responsibilities associated with managing nuclear material, one area of commonality among them is the need to be able to detect nuclear material, identify it, and quantify how much is there. This relies on nuclear material measurements. Nuclear material measurements assist the entire nuclear industry in being able to help manage its materials.

Santi then presented a schematic idea of what a generic LEU fuel fabrication facility would look like (see Figure 1-1). Such a facility converts uranium—usually UF_6[23] gas into fuel pellets—that can be used in fuel assemblies that are loaded into a nuclear reactor.

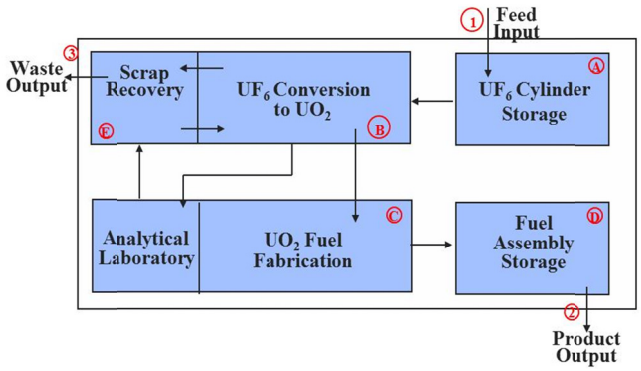

FIGURE 1-1 Generic LEU Fuel Fabrication Facility. SOURCE: Santi, 2012.

[23] UF_6 is uranium hexafluoride, the chemical form of uranium used in the enrichment process.

In the far left corner of Figure 1-1 there is a UF_6 cylinder storage area. Before accepting material at a facility, one has to ask the question, "How do I know the material has not been tampered with or somehow disturbed during the transportation process?" Changes create what is known as shipper-receiver difference. A measurement is needed when items are received to ensure that the facility sent the intended materials and that the items received are those that the shipper sent. Measurements may be as simple as weighing the cylinders or simply counting how many cylinders were received.

Depending on the value of the material and how much of a threat that material may cause to the public, one additional step may be needed, such as measuring a property associated with the UF_6 to ensure that the material received has the same properties as those requested (e.g., if the shipper said it sent 4 percent enriched U-235 in those cylinders, measurements may be needed to confirm that 4 percent enriched U-235 was received). In this case, a gamma-ray measurement may be taken using a gamma-ray detector next to the cylinder wall. This increases confidence in the ability to move material between facilities. To account for all the material within the facility, one must account for how much came into the facility by either relying on shipping records or on individual measurements on behalf of the facility manager. All materials measurements have some inherent uncertainties, depending upon the measurement technique used. Accounting for these uncertainties must be propagated throughout the entire material accountancy and management chain. Further, depending on how often accountancy is done at a facility, these cylinders may be measured again at some point.

In the scenario represented in Figure 1-1, the material has come to the facility to make fuel for nuclear reactors, and it will eventually be moved to another place in the facility where the UF_6 gas will be converted into uranium oxide power, UO_2. That process involves chemistry and there will be some losses within the pipes and other equipment associated with that conversion process. There will also be some scrap and other materials that go to scrap recovery and waste output. Some of that uranium will be accounted for as part of the material accountancy process. The vast majority of the material will be utilized in Part C of the schematic (Figure 1-1), fuel fabrication. The uranium oxide powder in various cans will be sintered and turned into fuel pellets, which are loaded into fuel rods that are in bundled into fuel assemblies that make up the reactor core.

In the schematic, there is another line going to an analytical laboratory. The fabrication process is not perfect, and measurements are needed within the facility to account for these imperfections. Those measurements on samples are conducted through destructive analysis, where chemistry is used to determine exactly how much enrichment and how much mass is associated with the oxides created. The chemical processes also create waste and leave the facility.

Throughout this whole facility, there are measurement opportunities to provide the facility management with the appropriate understanding of the location, quantity, and form of the material for tracking and management purposes. To account for and manage this entire process, multiple measurements are required—from simple item counting to complex gamma-ray measurements or

neutron measurements or destructive analytical chemistry measurements—to ascertain how material is flowing into the facility and how much material is accumulated in the facility.

Nondestructive assay measurements can be used to confirm enrichment levels for criticality safety. The amount of material that stayed behind in the equipment used for UF_6 conversion to UO_2 is known as nuclear material holdup. This can create criticality concerns if there is sufficient material in the wrong configuration. Nondestructive assay measurements are therefore conducted to determine how much is left in the pipes. These measurements aid both nuclear safety and accountability. They also provide input into management of nuclear security by helping to determine how much material is in a facility at any given time.

Santi then defined key terminology. An accountability measurement, he stated, "is a measurement to establish the special nuclear material mass value used in an accountancy system for a given item. These are normally high-precision measurements." The goal is to get about 1 percent or less uncertainty on the mass number for a given item measured. While that is a high degree of precision, if a facility has a sufficiently high throughput, this could, over time, lead to kilograms unaccounted for in a year-in/year-out facility. Note, this is material "unaccounted for" and not "lost." The material is still within the facility, in holdup, for example, but one simply cannot know exactly where it is at any given time without doing a full clean-out.

"Verification measurements," Santi explained, "are measurements to positively verify that there is special nuclear material content in a given item. Precisions are about 1 to 5 percent." The example of the shipper-receive measurement is a verification measurement. A "confirmation measurement" is a qualitative measurement taken to confirm that an item is marked correctly. It can be as simple as item counting. It could be weighing. It could be a measurement done relatively quickly simply to confirm that the item is what it is thought to be.

Nondestructive Assay Measurement Techniques

Santi then focused specifically on nondestructive assay (NDA) measurement techniques. These are techniques which measure a property emanating from the special nuclear material item or assembly of interest that do not force the contents of that item to be disturbed. The properties of the item are determined based on measurements external to the item. He chose to focus on NDA because it is most relevant to nuclear security discussions, since these measurements are used in portal monitors or anything used external to the facility to ensure knowledge of what could potentially leave through unauthorized paths.

There are basically three different NDA measurement techniques. The first is gamma-ray spectroscopy, where the emission of gamma-rays from the material is used to identify its properties (composition). For example, is the item low enriched uranium or highly enriched uranium (HEU): is the item plutonium or

uranium? Gamma-ray spectroscopy will indicate if the item is a simple source, like a cesium source, or if it is a special nuclear material.

Neutron counting is the second NDA technique, which allows one to determine if items are fissioning and at what fission rate. This provides a quantitative estimate of the amount of material in a given container.

The third NDA technique is calorimetry, which is measurement of the heat from the item. All radioactive materials, as they decay, produce thermal heat and that thermal heat can be used, when measured, to determine accurate quantities of associated mass, especially when measuring plutonium or large amounts of HEU.

By combining the information from gamma-ray spectroscopy, neutron counting, and calorimetry, one can determine quantitatively how much nuclear material is in a given item. It is important for accountability to keep track of exactly how much is going from/to different locations and in different configurations. Although a combination of the three techniques is best, even by conducting gamma-ray spectroscopy and neutron counting, control can be better maintained.

Nondestructive assay measurements have several advantages over destructive analysis measurements:

- they normally produce faster result (results within a few minutes),
- measurements can be performed wherever the material is located, and
- no waste is produced and the material is left undisturbed.

Santi noted that there is a role for destructive analysis (DA) in nuclear material accountancy because it provides higher-precision measurements allowing for better accountability numbers. Destructive analysis is better for measuring very small quantities of material: whereas NDA is probably sensitive to gram levels of material, DA is sensitive to much smaller quantities.

NDA is useful in nuclear material security in multiple ways. For example, if a portal monitor is set off, a nondestructive assay measurement will provide more information about what radioisotope caused the alarm. This can help distinguish between causes that are of concern (material illicitly leaving the facility) and those that are not of concern (an employee who underwent a nuclear medical procedure).

NDA is also helpful for domestic safeguards (as distinct from external or international safeguards). At Los Alamos National Laboratory (LANL), for example, NDA measurement is the most frequently implemented measurement technique to reliably determine the characteristics of special nuclear material. In the 1990s, approximately 65 to 75 percent of all Pu inventory measurements were performed with NDA techniques because they can continuously confirm what the inventory is, update the numbers, and provide accountability numbers. Specifically, NDA can play a role in:

- Accountability: determining the book value of a quantity of material in a given item or a given container.

- Confirmatory measurements: ensuring that items that cross boundaries from a material balance area with one set of accounting in one area of a plant to another have consistent values and that the items have not been tampered with since the last measurement.
- Shipper-receiver measurements: ensuring that material passing back and forth from facilities remains the same.
- Process control measurements: ensuring that a process using nuclear material is working appropriately and meets the appropriate quality standards, and that the material will perform to specifications.

Santi underscored that there is always a need to maintain a balance between nuclear security concerns and the ability to use the material. If nuclear security requirements become so onerous that it is simply impractical to work with the nuclear material, the material will not be of value. Using technologies and techniques and material control and accounting to balance and complement nuclear security is a way to maintain as much control over the nuclear material as possible, while still being able to use it for its intended purposes.

Another important issue to remember when dealing with NDAs is that if improper measurements are performed, if erroneous results are received, if there is an inappropriate error bar, or if errors are not accurate with respect to an item, there may be safety implications, especially criticality safety implications. These errors could also have security implications if nuclear material is lost and not detected. Finally, errors could have economic implications if a facility's resources are continuously utilized to re-measure items that were improperly measured the first time. To avoid errors, personnel within a facility must be able to make these measurements, which requires that they have not only training in how to operate a piece of equipment, but also knowledge of fundamental physics.

Improperly operating portal monitors or improperly trained personnel unable to understand what those portal monitors are detecting or monitoring can lead to other types of errors such as high false-alarm rates, which can lead these alarms being ignored, or if the monitors are not working properly, material may not be detected as it passes through the portal.[24]

Improper implementation, execution, and interpretation of NDA measurements can lead to a wide range of consequences that can potentially impact the safety or security of a facility. It is up to the personnel who are performing the measurements, ranging from the people who operate the equipment to the professionals who analyze the measurements, to ensure that an NDA measurement is performed properly by taking into consideration a number of different

[24]Portal monitors are examples of unattended measurements that are just kept on, running, and they alarm when there is a problem. Attended measurements, which are typically used to determine quantitative information, are taken within a facility to determine how much material is within a given item or a given canister. These types of measurements typically require trained personnel to perform and analyze these measurements.

factors. This includes how an item is packaged, the background radiation levels of the facility, and others.

Santi underscored that not all nuclear facilities are alike. Reactors and other facilities that contain large amounts of material receive a great deal of attention. There are various other facilities that have a smaller amount of nuclear material, such as universities. While it is important to secure this material, a graded approach is best. A university that has a very small amount of nuclear material cannot be treated the same way that a nuclear reactor with a very large amount of nuclear material is treated. Material measurements, then, can aid in developing security strategies. Therefore, in-laboratory or in-field training experiences working with real nuclear materials are important for personnel as they learn techniques and the principles associated with performing these measurements.

Effective training programs may be needed to develop or expand a person's knowledge and experience with fundamental physics associated with the specific NDA techniques they will be using. This does not mean that all technicians should be trained to become scientists. Principles can be taught that one can remember through lectures and laboratory experiences that become the foundation to build their skills to perform NDA measurements.

A training program needs to discuss not only what a measurement technique can and cannot measure, Santi said, but also with what accuracy and precision they can be measured. It is counterproductive to have someone make a measurement and indicate that the measurement is accurate to 1 percent when it is really only accurate to 10 or 20 percent, or that an NDA measured an item that was 50 grams when the technique was not developed to measure that type of item at all, and it is actually 500 grams. Having the knowledge of what the limitations are for these measurement techniques is important, as is the knowledge of how to properly calculate the resulting uncertainty and present that appropriately.

The training program that Santi directs began in 1973 and has trained individuals who work throughout the Department of Energy complex on how to perform measurements on nuclear materials for accountability. IAEA inspectors began participating in these training courses in 1974, and by 1980 IAEA felt it was so effective for their inspectors that LANL started a dedicated training program for them. Since 1980, every new IAEA inspector hired by the agency has traveled to Los Alamos to learn about the basic principles associated with nondestructive assay techniques, why the technique works, and where it does not work. These programs are customized, which means that if a person just works in a reactor facility, training is focused on that type of facility. The courses utilize an extensive inventory of nuclear material standards, including pure and impure plutonium standards, uranium standards, fresh fuel assemblies, and MOX standards.[25] This allows students to see and receive real data, and have

[25]A material standard is an object made to exacting specifications (composition, in this case) so that it can serve as a reference point for measurement of other materials.

real experiences in doing the measurements. Since its inception in 1973, LANL has conducted more than 315 courses for about 5,500 students. This has been a successful, ongoing program that continues to produce high-quality results.

In summary, effective nuclear measurements of nuclear material are necessary for the safety, security, and domestic safeguards associated with a facility that uses nuclear material. Performing high-quality measurements requires that the personnel involved in these measurements are appropriately trained, appropriately educated, and that training will then ensure a process of accounting for and securing the nuclear material that is as effective as possible.

DISCUSSION

During the discussion period, a question was raised about the need to educate the public on various degrees of risk from different types of nuclear versus radiological materials. Rajaraman suggested in response that the public must learn to distinguish among these risks, but because this may be difficult, he suggested beginning with explaining the relative risk from radiological materials. In part this is made more difficult in India, Rajaraman noted, because "for 50 years, we have been training them to be afraid of nuclear materials. It served us very well because it provided us with a nuclear taboo… Now you're to tell them, yes, be afraid, but don't be that afraid. This is a difficult and more delicate exercise, but it has to be undertaken if civilian nuclear energy is to survive."

A workshop participant asked Santi about the relative accuracy of NDA versus DA measurements. Santi replied that research is constantly being conducted to try to reduce the errors of NDA to near zero, or at least much closer to those of DA. He then provided the example of calorimetry of plutonium, which is the more accurate and precise NDA method for measuring plutonium. While one can get down to less than 1 percent or less than .5 percent accuracy, there is a trade-off in time. Calorimetry takes hours for measurements rather than minutes.

This points to another challenge, explained Santi. Researchers continue to try to reduce the amount of materials unaccounted for (MUF) to zero because the material is actually not lost, it is just impossible at present to account for it all. Likewise, there is a high degree of uncertainty about accounting for materials in nuclear waste. Despite efforts to reduce the amount of plutonium or uranium that goes into waste, one cannot eliminate it entirely. MUF, therefore, presents an on-going challenge to facility operators.

Another participant picked up on this point and noted that the challenge of trying to reduce MUF would be an interesting area for cooperation as would the entire issue of measurement control, bringing in the questions of how uncertainties combine, and which measurement methods are particularly problematic. All of these areas challenge experts in both the United States and India because there are really no good answers except additional research.

Santi was asked about NDA and sampling. He confirmed that there is no sampling with NDA; the entire item is measured. Because the entire item is

sampled, the only issues of accuracy come from the ability to interpret signals from the neutrons or the gamma emissions coming from the item. This requires measurement standards to understand how much bias is coming from the system that could cause inaccuracies in measurement.

This reality is replicated in training. Students are shown how the system works in an appropriate situation, where everything works properly. Then the situation is perturbed to show what off-normal situations look like so that students understand when the measurements are not accurate anymore. Essentially what training comes down to is understanding upset conditions and understanding when the situation is not perfect, which is why training should be done in a real laboratory. Realistic situations can then be used as teaching moments, and those are the best ones to have so that students have situational awareness when they perform the measurements.

A participant suggested that Indian scientists and experts would be enthusiastic to work with their counterparts from the United States on NDA, and one suggestion provided by a U.S. participant was to develop additional ways or techniques to help further establish the pedigree or the accuracy with which measurement standards are defined and/or characterized.

The session closed with the remark of a participant who underscored the desire on both sides to collaborate further in these technical areas.

2

Systems Approach to Security at Civilian Nuclear Facilities

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- Weapons-usable material must be kept out of the hands of adversaries who may be trying to get their hands on this material and could use it for malevolent actions.
- No material is absolutely safe, and any material is vulnerable at some level.
- Nuclear security is a continuous, dynamic risk management job and requires constant and vigorous efforts.
- Program resources were to be used for both safety and security. The balance of risk and security as well as the balance of resources needs to be maintained to not undermine employees' interest in maintaining high-quality science as well as a vigilance of safety and security measures.
- In India, the primary security concern at civilian nuclear facilities is sabotage.
- Several safety features can be incorporated into reactors, which also aid security.
- Material categorization is also essential to the security design process because there is a direct relationship between the protection required and the quantity of the material and its enrichment level.
- Apart from resource extension, the closed fuel cycle can be designed to be more proliferation resistant.

Promising Topics for Collaboration Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions do not necessarily represent the consensus of the participants, but are rather a selection of the topics offered by individual participants throughout the presentations and discussions.

- There is little sharing of experience among experts working in fuel cycle facilities in some countries, which indicates that there is opportunity for communication in this area.
- Due to the high consequence to the public if a malevolent act were to occur, proper protection planning, design, and implementation approaches are well documented and shared within the global security community. However, thus far Indian and American experts have not had an opportunity to fully exchange experiences, therefore more such opportunities should be sought bilaterally and within the broader security community. This offers the opportunity for more Indian-U.S. exchange.
- The problem of how to assess quantitatively the probability (frequency) of attack in the security and safeguards areas may be one possible joint research project.
- Commonality in the measure of consequences across safety, security, and safeguards is a possible area of joint cooperation.
- At many nuclear installations there is a need to augment communication resources for purposes of both security and safeguards.
- Consequence management training tools, such as the development of a plume simulator for handheld instruments, could be another area of cooperation.
- Exchange programs for students would be beneficial for both countries.

Overview of Civilian Nuclear Security: A Systems Approach

Robert Kuckuck drew upon his experience as a former director of a nuclear facility and a principal deputy director of the National Nuclear Security Administration to provide his views on security for civilian nuclear facilities from a systems perspective. This perspective begins, he stated, with a global system and continues to the local, facility system. The global system involves policies and agreements; the domestic system also involves policies, enforcement, and oversight. Operational facility systems are embedded systems that involve the actual handling of materials and the actual implementation of nuclear security features.

Nuclear security systems from a facility and operational perspective have always had two principles for Kuckuck. The first principle is that weapons-usable material must be kept out of the hands of adversaries, and that adversaries are indeed trying to get their hands on this material and could use it for malevolent purposes. Responsibility for protecting the mateiral is the utmost priority.

Even though there has been a tremendous global effort over many years, there still are no agreed upon standards around the world for protecting nuclear material. Any individual state is only as safe or protected as the weakest link in the entire international system. A systems approach is very much needed on a global level. Kuckuck noted that dialogue among scientists is an important first step, and many, many more steps between India and the United States are needed. Scientists start with facts that are well understood on each side, and can make progress in forming understanding relationships and developing a path to the future.

Kuckuck's second guiding principle throughout his career was that no material is absolutely safe, and any material is vulnerable at some level. Therefore, the task of nuclear security at the level of facility operations has always been one of risk management. How does one assess the quality and quantity of the material at the facility, and how does one assess the attractiveness value of that material to an adversary? What security measures are in place to protect that material? And what is the understanding and best estimate of the capabilities that an adversary can bring to bear against the facilities and operations? It is the balance of those factors, the risk management, that constitutes the nuclear security system at a facility-operations level.

All of these factors are dynamic, continually changing and uncertain. The capabilities of security measures change. The perception of the adversaries' capabilities changes. The public's perception of security measures and the adversary's capabilities are every bit as important as the facility director's understanding of the facility in real time. These are very real concerns to a facility manager, and particularly to a government official. This continuous, dynamic risk management job, which is what Kuckuck calls nuclear security, requires constant and vigorous efforts.

With these two principles, the facility director concludes that he or she always has to have his or her eyes open and mind active to decide if the balance of risk is appropriate.

To Kuckuck, the most important and fundamental element of facility security is the people. The security culture of the facility is critical to the effectiveness of the facility's security system. A facility's management has to convey and communicate a need for the security measures in place, "not just walk the walk and not just talk the talk, but to walk the talk." Management has to act in support of those principles at all times with an organization structured with clear motivations, incentives, roles, responsibilities, accountabilities, authorities. Every person must be trained to know why they, and management, are taking these measures. The people must have the authority and the capability to do their jobs,

including the resources they need. If any of those conditions are violated, management loses an employee's support; his heart is no longer in tune with the principles and this starts to weaken security culture. As a facility director, Kuckuck always felt that one of his biggest jobs was to maintain and sustain that security culture at his facility. Every person, from a custodian to a technician to a scientist to the protective force guards, needed to believe in and support the nuclear security program. That is what Kuckuck calls nuclear security culture.

There are many other elements in the nuclear security program at a facility with attractive nuclear material, be it a reactor, a materials processing facility, or a storage facility. Kuckuck began by asking himself if the facility was robust. Can the facility process the material, handle it, store it, take care of it?

The second element was how much material was at the facility and how should it be controlled and kept track of? How does the facility director know at every minute whether the material is still there? How does the director know that something hasn't gone wrong and that nothing was missed or that material has not gone missing? To answer these questions, Kuckuck employed material control and accountability.

Next, he asked, "How do I control people's access to the material?" The answer was to put up barriers. In the United States, facilities commonly have several concentric barriers of increasing magnitude. Outside barriers may not even be alarmed, merely patrolled. As one moves inward, toward the material, the barriers become much more robust. They are alarmed and are constantly monitored. This layered system is called a graded approach.

As one moves in, one reaches a hardened facility with even stronger barriers. At this level, access is controlled for each person. Each person's motive and authorization for being in that zone is diligently investigated and understood. Each person is given credentials, which are the only way that he or she can access the secure zone. In some cases, individuals are allowed access, but must be accompanied by more than one person, use more than one key, and use more than one control system.

Now that the facility has the material controlled inside, and has only granted access to the right good guys (and there are lots of other good guys that are not granted access), how does the facility keep the bad guys out? This begins with surveillance. Barriers are monitored constantly, as are alarms. Protective forces are engaged and conduct patrols, and the like.

If an alarm signals or if there is some indication of a penetration of a barrier, or an attempted penetration, facility personnel, especially the protective force must be prepared to respond immediately. In some cases, additional barriers go into place automatically. Communication occurs across the entire facility so that everyone knows that there is an issue, prompting them to lock up their own material or do whatever is appropriate in their position. The protective force has an even more thorough communication system so that they know exactly what is happening at any point in time and can adjust their reactions accordingly. Finally, a pursuit and recovery operation is undertaken to either contain the intruders and/or recover the material. If needed, each facility has

very prescribed ways in which the protective force reaches out to supplemental forces such as the local police, the military, etc. As a facility director, this was the system that Kuckuck always had in his mind as he reviewed security.

However, he observed that there are at least three very important elements that underpinned this sequence of protections just outlined. The biggest one is the human aspect of nuclear materials security. Every person who is involved with the material system at any level is completely vetted with background investigations. This occurs every five years at a minimum. Employees are not vetted by the facility or by the director, they are vetted by an independent government authority so that there is no chance for conflict of interest by the director thinking he needs a particular individual and maybe does not do the investigation diligently.

Training is required in every aspect that is relevant to protecting the material during handling, storage, and so forth. Fitness for duty, which is different from training, is a daily inspection done in various ways. For example, for the protective forces, the supervisor of a small group on each shift does various tests or interrogations to make sure that every member of his team is fit for duty that day, is not sick, or does not have some other issue that may prevent him from doing what he needs to do.

Technology supports all of this, whether it be offensive or defensive weapons or alarms or capabilities. A major aspect of this technology is cyber-security, both in the control and communications of the facility. Forensics also plays an important role in deterrence and resolution should an incident occur. One hopes that an adversary is deterred by the concern that he will be caught and brought to justice.

Finally, another underlying technology is just information security in general. Across the whole facility, how does the facility protect information that pertains to the classification of material, the location of the material, and how the material is protected. How is the information protected once it is classified? These are underpinning technologies, or underpinning elements, that are fundamental to the system of nuclear security at any facility.

Kuckuck then shared issues that arose during his time as a director of a facility and as a government official overseeing these facilities. One of the biggest difficulties as a director of a facility with nuclear operations was sustaining the nuclear culture. It is a constant task and there are many realities that try to undermine that culture. One is just plain complacency: years go by and no intruders come through the fence and there are no issues. If we lose the hearts and minds of the facility employees regarding the need for security, then they start doing that risk balance on their own. They start deciding that they do not really have to do a lock up or take a compensatory measure because it is not necessary. It is very important to not allow the security system to get into the position of being judged by the employees in a critial way that allows them to make their own risk balance. Complacency is a very serious issue.

Resources are another important issue. As a director, there is a constant balance required between using resources for the mission with the material and the security required to protect that material. That balance can be off in either

direction. Some people will argue that one cannot have too much security. But Kuckuck believes one can have too much of the wrong kind of security. This applies to safety as well. There may be multiple requirements for bureaucratic accounting of things that make no real contribution to safety and this begins to undermine the safety culture itself because employees become disgruntled and they do not follow the safety rules or they fake it or they just do not take it seriously.

The same thing happens with security, therefore it is important to maintain the balance of security requirements and actual risk. This requires the development of a design basis threat (DBT), which is established by government oversight organizations. Specifically, they define the threat that the facility has to use as the basis from which to build its nuclear security. The DBT is derived by using intelligence, understanding of an adversary's past actions, and other input.

Kuckuck explained, however, that there is a cycle to DBTs. A force-on-force exercise, bringing in so-called armed adversaries to attack the laboratory, would be conducted to determine whether the security system could meet the DBT. If the laboratory forces defended every time successfully, the people that designed the threat felt that maybe they needed to escalate the threat a bit. They wondered where failure would occur: perhaps if the adversary had one more machine gun? Therefore, the laboratory would test beyond the DBT, and test to failure. Invariably, however, that would become the new DBT. This created periods where the DBT was totally out of alignment with realistic threats from an adversary. When that happened, people would start to lose adherence to the security system. They knew the threat was not realistic, they were bitter, and they made their own judgements. The situation also could go the other way. Program resources were to be used for both safety and security. The complacency factor would enter and resources for security would be cut. As stated earlier, the balance of risk and security as well as the balance of resources needed to be maintained to not undermine employees.

The second issue is very difficult. Kuckuck explained that in the United States, facilities are not guarded by the military, they are guarded by security companies or employees of the facility. These people must be trained. Most guard forces are recruited from among soldiers returning from Iraq or Afganistan. But they come home and complain that after a little while, they feel like night watchmen although they are expected to be soldiers, to train like soldiers, and to do combat exercises. They drive a car around all evening and nothing ever happens. It is very difficult for them to adjust to that, it is very difficult to keep them alert. There have been incidents when guards missed obvious events that were not even an exercise, someone trying to cut through a fence, for example.

Another significant problem is the degree to which the exercises are realistic. During a major exercise at a laboratory, there is a full security force on site right then that are not playing in the exercise—they are protecting the facility. There is another shift that is going to be exercised that night and they all

have yellow vests on and are using laser guns to shoot each other in the vest. There is a vast number of people out here in the yards: some are umpires, some are judges, some are observers, some are guys with vests who are playing, and some are guards that are ignoring them. It is very hard to have a realistic exercise of troops. Kuckuck has always worried about that problem.

Recently there was a situation in the United States, Kuckuck recounted, that raises a question about threats. An 82 year old nun and a couple of other gentlemen cut through the fence and entered a facility. In analyzing that incident, many of these factors came into play. They never actually got near the material and there was never a real threat, but there were a lot of lessons to be learned from how this happened.

Regarding accountability, as a facililty director, Kuckuck found it very difficult to explain to the public in the United States why the fact that kilograms of highly enriched uranium (HEU) or platonium would go "missing" every year is considered unclassified information. The material was held up in the pipes, or otherwise unaccounted for (see Santi's talk). The argument of course, is there are ways that one can eventually account for that material by decontamination. This was a very difficult public relations issue.

Kuckuck concluded by asking "Are we using technology to our fullest extent?" He answered, "we know we are not." There are more aggressive deterrence capabilities that could be automatically activated when someone came through a fence, but this may lead to an accidental killing, which underscores the need to balance safety and security. Are there other technologies not being used to either inhibit the intruder or to devalue the target they are coming after? Is there artificial intelligence that the guards can use to help them in their boredom so that they don't miss something on the camera?

NUCLEAR MATERIALS SECURITY AT CIVILIAN REACTOR FACILITIES

Indian Perspective

Ranjit Kumar shared his experience working with civilian nuclear facilities in India and the associated issues of nuclear materials security that he has encountered. He began by noting that in addition to pressurized heavy-water reactors, which have been the mainstay of the India nuclear power program in the first stage of its development, India has developed advanced heavy-water reactors, which are based on low enriched uranium and thorium with several improved safety and nonproliferation or proliferation-resistant features. India also has a program on fast breeder-type reactors, with a research reactor now running for nearly 30 years. Also, India's prototype fast breeder reactor will be ready in a couple of years.

India has various types of nuclear facilities encompassing the entire nuclear fuel cycle, starting from mining to power production and other uses of

nuclear radiation sources, to waste disposal. India has both back-end and front-end fuel cycle facilities in the civilian domain.

India is poised for extensive growth, including potentially the use of many more nuclear power reactors in the country. As nuclear power reactor deployment increases, there will be increased requirements of fuel fabrication and other fuel cycle services. Non-power applications of radiation are also growing across India, particularly in industrial and agricultural applications. There are large programs that have made a contribution to the overall economy of the country.

Regarding security at civilian nuclear facilities, the primary concern is sabotage. There have been several terrorist incidents that cause concern about potential sabotage attempts on a nuclear power plant, other civilian nuclear facilities, or any nuclear facility. These concerns have led experts in India to look deeply at the security of these facilities including various analyses right after the attacks of September 11, 2001. A review committee was established to look into security. Subsequently, regulations were developed and a great deal of oversight, audits, and reviews have taken place. Immediate measures have been undertaken and long-term goals have also been developed. Several design-related measures have been introduced in order to prevent and protect the nuclear facilities against sabotage attempts.

Although sabotage is the primary threat, theft is also a concern, not as much for nuclear power projects or nuclear power facilities or power reactors and research reactors, but rather for other facilities such as fuel fabrication facilities. Facilities such as reprocessing facilities have both sabotage and theft threats. As an end product, reprocessed material may be a theft target.

Kumar provided some examples of nuclear facilities and comments on their potential as sabotage targets:

- Nuclear power plants:
  - core damage or containment failure, which can lead to radioactive release
  - spent fuel storage: pool could be drained and lead to radioactive release
- Research reactors:
  - target depending on the type of reactor
- Fuel fabrication facility:
  - not a primary sabotage target, but could be even though it will not cause consequences as severe as a sabotage attack on a facility with radiological materials or a reactor facility
  - end product can be utilized to cause a disruption as well as to contaminate an area
- Enrichment, conversion, and storage facilities
  - spent fuel reprocessing facilities and waste disposal facilities are of greater concern
  - in a waste disposal facility, there is a heavy concentration of materials that may present a potential sabotage target

Based on International Atomic Energy Agency (IAEA) data, there have been attacks on facilities, and in many cases the aim has been sabotage. In some cases, theft was the motive. Kumar noted that India wants to avoid such incidents.

Attacks can take place in three major ways: stealth, deceit, and force. Physical protection systems should address all three methods of attack. That said, Kumar noted that civilian nuclear facilities, particularly reactors, are difficult targets for sabotage. There are several safety features incorporated into the design of the reactor itself. Specifically, he referenced several fundamental principles of design safety:

- Redundancy: ensure that safety does not depend on any single system functioning correctly
- Reliability: design to numerical reliability targets (999/1,000)
- Testability: ensure systems are testable to demonstrate their reliability
- Independence: ensure systems that perform the same safety function are independent
- Separation: ensure systems that perform the same safety function are spatially separated
- Diversity: ensure, where possible, that systems which perform the same safety functions are of dissimilar design
- Defence-in-Depth: multiple barriers and systems
- Fail safe: ensure system/component fails safe if practical

Kumar elaborated on the principle of "diversity." For example, in a nuclear power plant shutdown system, there are diverse mechanisms or diverse methodologies used for this purpose alone, such as a cooling rod, which uses a neutron-absorbing material like cadmium. There are others, like injection of neutron poison into the coolant. Several such diverse mechanisms are utilized for safety purposes in order to address that single failure and ensure that the plant remains safe.

Many of these safety features also aid security in diverse ways. For example, to release radioactivity from a fuel core in a pressurized heavy water reactor the radioactive material would have to breach the fuel cladding to enter the coolant tube and then to the reactor calandria vessel, to the biological shield, which contains the leak. This all makes the reactor a hard target for sabotage, although the risk cannot be entirely eliminated. Risk can never be 100-percent eliminated.

New, evolutionary reactor designs are bringing security into the design drawing room itself to attempt to incorporate security features, which will aid security directly. This is known as security by design. This process begins with siting and continues to the design of the containment facility, and throughout the entire process. When considering security measures themselves, if they are incorporated into the design phase, they are significantly more cost effective than attempts to retrofit a facility. At times, certain security measures are impossible to retrofit.

The Indian nuclear power program is guided by certain regulatory prerequisites overseen by the Atomic Energy Regulatory Board (AERB). The AERB is responsible for oversight, as well as for all aspects of review and audit of plants already in operation and those in the design phase. Each plant design is reviewed for its applicability, maintainability, and upgradability, particularly if it is an existing operating nuclear power plant. These designs should be consistent with national and international guidelines, standards, conventions, and treaties. Kumar noted that India follows certain international guidelines, particularly those stipulated by the IAEA and other regulatory bodies. Experts in India try to understand the requirements and to compare and adopt similar policies as well as design philosophies most suitable for India.

The main elements of security at nuclear facilities include security organizations with a well-defined allocation of responsibilities, duties and reporting lines, and well-coordinated with state agencies. The following questions are answered by these organizations: What is the responsibility of the guard force? What is the responsibility of the security manager or the chief security officer? Whom should this person contact in local law enforcement agencies?

The next element of security is the engineering system for physical protection. This includes hardware systems such as fences and barriers, detection and alarm devices, access control and surveillance, and guards. The physical protection system is designed based on the performance of the guard forces and the design basis threat (DBT). These aspects of physical security all interact. Kumar noted that they are trying to analyze response times and appropriate response forces against the DBT. Contingency and emergency plans are also designed for both security and safety. This is a systems engineering approach that can be utilized for the physical protection of any critical infrastructure facility.

This process starts with the required analysis stage even before the design of the reactor, during which the target is identified in vital areas. This vital area identification is a separate process in itself because it is essential to determine protection equipment needs, with particular attention to the threat of sabotage. A detailed methodology is followed in this process to determine a minimum set of locations and equipment needed to provide full protection against sabotage and the release of radioactive materials. In particular, during the identification of vital areas, two sabotage scenarios are considered. The first scenario is a "direct" scenario during which adversaries sabotage the material itself (e.g., using explosives) with the aim of causing radioactive dispersal. In such a scenario, an adversary would use some explosives. The second scenario is an indirect one during which a safety system would be attacked causing the dispersal of material. Kumar stated that this is called an event of "malevolent origin" and the security systems—through the DBT—are designed to prevent such events, again, starting with the vital area identification process.

Material categorization is also essential to this security design process because there is a direct relationship between the quantity of the material and its

enrichment level with regard to vital area identification, although categorization of material does not factor in with sabotage threats. Kumar stated that there is an effort in India to categorize nuclear facilities from the point of view of radiological sabotage but it has not yet been established. There are efforts to define criterion for what is called an "unacceptable radiological consequence" (URC). Each state in India is to define what an URC would be and based on that definition, the vital areas to be protected would be defined. However, the physical security at a nuclear facility should protect against any sabotage scenario even those exceeding the URC criterion.

A design for these scenarios would follow the same principles of detection, delay, and response, which are interlinked. Until the detection takes place, there is no value of a delay. This systems engineering methodology brings in two competing timelines. One is called the physical protection system timeline and the other is the adversary timeline. In order for the adversary to be successful, he has to complete his task before the physical protection system (PPS) delay time. If the task completion time by the adversary is more than the PPS response time, then the security system is successful. To establish these timelines, the first step is identification of the critical detection point, and a definition of the role of early detection.

The security elements of detection, delay, response, and access control are the same for a nuclear facility as well as for nuclear materials. A good security design should include:

- balanced protection: the front end and the back end of a facility should be protected equally
- protection in-depth: layered protection measures, not only physical measures, should be applied
- reliability: the instruments and systems should be reliable
- information security: should not be neglected
- confidentiality: physical protection systems should be kept confidential to maintain the reliability of the system
- consideration of operational needs: security systems should not interfere with the operation of a facility

There is considerable interaction between safety and security systems and at times, they have contradictory requirements. Such contradictions should not be allowed in the case of security. To address these issues, dialogue is needed between safety and security requirements.

Indian nuclear power plants, from the inside out, have four layers of protection, starting with the operating island. There is a double fence around the inner and the vital areas. This is called the protected area. Then there is the main plant boundary, the outermost layer is known as the exclusion zone boundary, the second layer is the main plant boundary, which is 500 meters from the operating island. Third is the operating island, which is declared as a protected

area. Fourth is the vital inner area, where the target for the sabotage or theft is located. They have their own required security measures.

In the exclusion zone boundary, there are manual measures for detection and assessment, such as patrols. In the main plant boundary, there are manual, and in some cases automatic, measures. In the operating island, there is a complete automatic perimeter intrusion detection and assessment system. In the vital area and the inner areas, there are automatic systems for intrusion detection.

Access control is done in a similar graded manner. In the exclusion zone boundary, this is done manually. In the main plant boundary, this is done automatically, with RFID smartcards. In the operating island, there are RFID cards plus biometrics. In the vital areas, there are automatic RFIDs plus biometrics in some cases. The physical protection system is integrated, and includes a central alarm station, located inside the protected area, that monitors all activity. This area has access control measures. Perimeter intrusion detection measures include frisking and checking in at the main plant boundary. There are also measures against forced entry of vehicles and civilians. Kumar stressed that all of these systems were developed indigenously, originating either at Bhabha Atomic Research Centre (BARC), Electronics Corporation of India Limited, or other similar organizations.

Again, while there is a synergy between safety and security systems, security is governed mainly by the Central Industrial Security Force and local police, particularly the response forces. However, safety is governed by the facility operator, the Nuclear Power Corporation of India Limited or Heavy-Water Board, depending on the type of facility. This system is quite mature, Kumar noted, whereas the security aspect, including the regulatory aspect of security, requires more time to evolve.

Since at times safety and security measures aid each other and at times they contradict each other, appropriate attention should be given to this balance. Both nuclear safety and security have the same aim: protecting the public and the environment from harmful effects of radiation. They also share a common regulatory approach by the same regulatory body. There should be synergy between safety and security. Addressing the need of the one by the other and understanding the requirements of security by safety and plant operation is important.

Regarding the regulatory framework, all nuclear power plants and civilian nuclear facilities are governed by AERB. At the design stage for new plants, there are several guidelines for systems design, inspection, and event reporting. This process is broken into stages and is followed as the plant develops. Quality assurance for equipment and systems is the responsibility of the operator. They are periodically reviewed and audited, including the response aspect. Several aspects of physical protection for civilian nuclear facilities are audited and reviewed by AERB regulations.

The right mix of hardware, security personnel, and procedures have to be utilized for effective physical protection of nuclear facilities. Kumar stressed that

several of the technologies used in India are developed in-house, but standardiza-standardization remains one of the requirements. The best available sustainable techniques and instruments should be used on a long-term basis because it is not possible to change frequently. Also, there is a requirement to connect with local agencies for additional support in an emergency. This is vital, particularly when off-site emergencies arise. Likewise, appropriate quality-assurance and emergency plans must be deployed and practiced. Kumar assured workshop participants that India's nuclear power plants deploy some of the most modern security systems and equipment. Good procedures are also practiced, reviewed, and audited. Often licensing is completed based on the security review and auditing. In closing, Kumar stated that it is also important today to include the neighborhood in the effective implementation of effective nuclear security.

U.S. Perspective

Michael Browne began by stating that his presentation would address nuclear material accountancy and physical protection, as well as focus on how the aspects of material accountancy in particular are applied to heavy-water reactors (CANDU facilities), including how standard measures are employed to achieve material accountancy. Browne also referred to supplemental measures that can be employed at reactors to gain confidence in the results from the accountancy systems. He concluded his presentation with a case study of the application of accountancy systems specifically to a sodium-cooled fast reactor to improve or enhance nuclear security.

The ultimate goal of nuclear security is to protect the public. Browne said that there are two ways to do this: protect against the malicious use of the nuclear material, and prevent the sabotage of nuclear facilities. At reactor facilities, nuclear security is implemented by using physical protections to control access, limiting access to those people who have a need to access the reactors, and the nuclear material accountancy system to keep track of the material and detect theft and potential misuse of the material.

Accountancy systems are typically developed based on the type of facility and should employ a risk-based approach, Browne argued. Because different types of reactors have different types and quantities of materials, different inherent accessibility, different operations, and different regulatory requirements, they require different accountancy systems. The tools may be the same, but the way that the tools are applied may be different.

Principles Associated With Material Accountancy

The most important principle, the backbone, is the accounting system itself. The accounting system can be viewed as the medium used to keep track of inventory. There is a wide range of systems, from handwritten notes in a ledger, to an electronic spreadsheet, to a fully interactive electronic database that tracks nuclear material in real or near real time, such as the system used in the facilities

in the United States, the Local Area Network Material Accounting System.

That accounting system typically utilizes material balance areas and key measurement points, MBAs and KMPs, as sources of information. For reactors, MBAs are the places where nuclear material is either used or stored. Key measurement points are used to determine the inventory in MBAs. For a nuclear power plant, a key measurement point might be a neutron monitor that is used to verify that a particular item is still in a storage configuration. It may be a gamma detector, which is used to confirm that a particular item has moved from one material balance area to another material balance area. Accounting may require actual material balance or an item count (e.g., number of fuel assemblies). In reactor facilities, item counts are typically used because the material does not change form. One knows the enrichment level of the fuel coming into a facility and the changes that occur in the reactor can be inferred from the operating parameters of the reactor. When it is ultimately discharged as spent fuel, the basic block, which is the assembly, has not changed, therefore item counting can be employed for accounting.

Application of Material Accountancy to CANDU Reactors

Browne then applied this concept of material accountancy, MBAs and KMPs, to a CANDU reactor to illustrate how this case differs from a more complicated one discussed later in the presentation.

For a CANDU facility, there are essentially three material balance areas: the fresh fuel area, the reactor itself, and the spent fuel storage pool. There are two types of key measurement points associated with those areas: KMPs for inventory and KMPs for flow. The distinction between them is that a key measurement point in an inventory is usually employed in a static configuration to verify that the inventory is as expected. If one had 20 items before, the key measurement point for inventory may be to go back and count the items to verify that there are still 20.

The flow KMPs are the record-keeping mechanism to keep track of material as it moves from MBA to MBA. The flow of material is such that the fresh fuel goes in through the reactor containment building, goes past a series of radiation detectors or monitors, is loaded into the reactor, and then, when it is discharged, takes a separate path out past a core discharge monitor and then eventually into the spent fuel storage bay.

How do these MBAs and KMPs work to form material accountancy for a CANDU facility? For the fresh fuel receipt and storage, the traditional measure is simply item counting. For CANDU facilities, one bundle is essentially a little less than 20 kilograms of uranium. There is no method today for inventory counting in the reactor core. Rather, accounting is addressed largely by the flow KMPs.

For spent fuel storage, the inventory key measurement points are essentially item counting coupled with some mechanism to verify that what is being counted is indeed consistent with irradiated material. The Cerenkov viewing device, a CVD or DCVD, is a typical example.

The core discharge monitor is a neutron and gamma tool that actually examines direct gamma and gamma-n reactions to give a unique signature that should be consistent with the known operating parameters of the reactor.

Next, Browne discussed some supplemental tools that one could apply to increase confidence in the nuclear security regime for these types of facilities. He then applied them to the sodium-cooled reactor.

The first is unattended monitoring systems. In general, an unattended monitoring system (UMS) is a radiation-based system designed to monitor the movement of nuclear material throughout a facility, whether the moves are intended or unintended. It can track fissile material or radiological sources by looking for specific characteristics that indicate the type of material, and it can compare the findings with the declared facility operations. If the operators know how the facility is operating, then the material movements detected should be consistent within that framework.

The UMS is usually designed according to the facility layout and what type of equipment is present to move the nuclear material such as cranes, entry points, exit points, and shielding. All of these items are factored in when designing an unattended monitoring system. Often a UMS pulls data from other sensors to provide a comprehensive view of how material is moving around and the activities associated with that movement.

Another supplemental tool is a near-real-time accountancy system (NRTA), which uses modeling and simulation tools to give the operator an idea of the real-time location of the material. Browne shared an example for a CANDU facility: As noted above, the operator knows the fuel's initial enrichment, and the operational parameters of the reactor, such as where the assembly is loaded, the total core burn-up, and the reactor core power profile. Based on these inputs, the operator can use depletion-code calculations to determine what the uranium and plutonium content of the fuel assembly is at the time of discharge. With that information in an NRTA system, the operator can track all the special nuclear material of interest for all of his assemblies. The NRTA system can be validated by taking a once-through simulation and comparing it against measurements either from NDA or analytical chemistry.

Containment and surveillance tools, such as cameras, tags and seals, and tamper-indicating devices, complement the accounting system. Cameras with attentive guards or an unattended monitoring system that records the information enhance security. Tags and seals, whether metal or digital (e.g., a fiber-optic seal) show that an item has been accessed and, in some cases, an indication of the time when it was accessed. If incorporated into a UMS system, a seal can also trigger alarms sent to the central alarm station for a response.

Finally, advanced material assay capabilities can be used if more quantitative information is required. This can be done either as a random sampling program, to instill confidence in the material accountancy system, it could be used just during inventory verification, or it could be used in times when an event has occurred and one needs to recover from a discrepancy.

Example 1: A CANDU Reactor

The movements of fuel in a CANDU facility illustrate the application of these different tools. As the fresh fuel is moved into the CANDU reactor, it moves past the core discharge monitor. Because it has not been irradiated, the fresh fuel is easily distinguished from spent fuel. The core discharge monitor often does not give a clear signature, which is why in this area there are two sets of radiation detectors that have a greater sensitivity to let one know that the fresh fuel has moved into the reactor area. They are also there to prevent the discharge of fuel back through this path.

As the fuel is discharged from the reactor after irradiation, it passes the core discharge monitor, giving a characteristic signature, and moved into the spent fuel storage area, where it again passes through some general radiation monitors, which provide motion detection and direction of motion over the general area. Finally, a series of cameras deployed throughout CANDU facilities provide surveillance. When the fuel assemblies are in a static configuration, the operators often will use tamper-indicating devices to make sure that nothing has been accessed.

Example 2: A Sodium-Cooled Fast Reactor

Browne then described the tail-end of a sodium-cooled fast reactor. Accountancy systems associated with this type of reactor facility are dramatically different than for a CANDU facility. The core of such a facility is located several stories up and the fuel is discharged into a spent fuel pond. There is a vehicle access area, a lorry hatch, which is used for bringing equipment into and out of the spent fuel area. There is a set of rail tracks, which goes into a lower area used for moving the spent fuel into dry storage. There are hot cells used for post-irradiation examination and for handling and repackaging of radiation sources. There is also a personnel access area to the spent fuel pond. A series of radiation detectors, as well as cameras distributed as part of an unattended monitoring system, are part of the security.

Why would a liquid sodium fast reactor facility require a dramatically different approach from a CANDU? Unlike a CANDU, where the fresh fuel is natural uranium and the output is very limited quantities of relatively unattractive plutonium, the sodium-cooled fast reactor uses fuel with higher enrichment (26 percent HEU in the hypothetical example given) and may be run to low burn-up, producing large amounts of weapons-grade plutonium. If a facility was at a heightened security posture because of external circumstances, a very advanced accountancy system would be employed to maintain a high level of fidelity on the location of the nuclear material. In such a scenario, a twofold approach would be utilized. First, all the material would have to be characterized exceedingly well and the characterization would have to be maintained for an extended period of time. Second, the material would have to be tracked continuously throughout the facility.

To address the first point in this design exercise, as the fuel was discharged each assembly was measured using an underwater neutron coincidence counter. Combined with information as to the initial enrichment, isotope composition, depletion code calculations, that coincidence neutron measurement yielded a total plutonium mass on an assembly-by-assembly basis. Then to address proliferation concerns, the six assemblies were repackaged together into a proliferation-resistant canister. This makes the fuel more difficult to steal because bundled together the fuel is bulkier and heavier, and it has a higher radiation dose rate at the surface.

In such a facility, an unattended monitoring system would be designed and installed to track the movement of this material and to make sure it did not go through the lorry hatch or was not pulled out through the hot cells up back into the reactor hull or prematurely taken out through the rail access point. This was implemented through a series of detectors, designed specifically to look for the characteristics of the fuel associated with a specific facility. One of the difficulties associated with this sample facility, Browne noted, is that it was also used in the construction and repackaging of radiological sources such as cobalt-60 sources, and cesium-137 sources for industry. It was also creating antimony beryllium and americium beryllium sources for the local oil industry. So the system had to be capable of differentiating between these movements and the movements of the fuel itself in an operational mode.

Cameras that recorded activity were incorporated into the security design at the hypothetical facility examined, but they were triggered by radiation events so as to not create copious amounts of video data that were difficult to store. There were also other sensors included in this design to monitor movement. There was a series of underwater detectors, which were designed to take a look at the places where the fuel could be moved out of the water, and incorporated with that were underwater cameras, as well as ultrasonic sensors to make sure that shielding was not moved in front of the detectors, thus obscuring the signals.

The data from this system was fed into two other systems, the nuclear material accountancy system, so that the operator knew, in real time, where the material was and could differentiate between the operations associated with the sources and the operations associated with the fuel. It was also fed into the physical protection system at the central alarm station.

In addition to these measures, Browne noted that at personnel entry and exit points controlled by the physical protection system in the form of turnstiles, the operator had the ability to lock out the turnstiles and then respond accordingly should a specific signature be seen. The set of signatures the system looked for was generated by considering different possible shielding configurations and, if necessary, a full spectral analysis. The systems were helium-3 detectors, fission chambers, ionization chambers, and sodium iodide scintillation detectors.

Integrating information from different types of detectors is essential. For example, one may receive video data, an operator declaration, and real-time data associated with either radiation detectors or other sensors. As an example, the operator might declare his/her location at a particular time, the material that

he/she is working with, the activity he/she is conducting, and who he/she is. What one would like to do is to correlate this with the other data that are being recorded to build confidence in one's knowledge of what is occurring. In this case, the video data will be watched and analyzed, looking for the time stamp, comparing it with the clocks, and looking at who is doing the activity and confirm it against the operator declaration.

At the same time, one should chart the signatures associated with the activity itself, for example, by looking at a door sensor to determine whether a door is opened or closed. The next step is a total neutron count. The third step is from a sodium iodide detector, which can measure with moderate resolution the energy and intensity of gamma rays and can infer enrichment and other aspects of the composition to make certain that what is being seen is a signature consistent with the declared material.

The idea is to pull all these data together in such a way that they provide increased confidence that the accountancy system is keeping track of what is occurring. In the example above, this was done through time synchronization of all the data generated by sources at a location. Associated with sharing data between a nuclear material accountancy system and a physical protection is the need to ensure that there is a consistent time base when trying to determine what is happening. In particular, if there is an inventory discrepancy to be resolved, having a consistent time base is critical.

Browne then discussed spent fuel. Currently, quantifying plutonium and spent fuel for security purposes is very difficult. It is not such a problem for the reactor, but it is a big problem for shipper-receiver differences, when the reactor ships it out to a reprocessing facility, and for input accountancy for reprocessing centers themselves. Currently, accountancy for spent fuel is, unfortunately, very simple. It uses Cerenkov viewing devices just to look for the Cerenkov signature or it uses detectors to confirm the presence of cesium-137 or fission to observe.

Recently, the U.S. Department of Energy and the National Nuclear Security Administration decided that they are going to take on the challenge of trying to improve the ability to directly measure plutonium content in spent fuel. This project is a several-year effort that is designed to examine the most promising technologies for the measurement of spent fuel, narrow that set based on agreed criteria, and then design and deploy the detectors to international partners around the world with whom the United States conducts spent fuel measurements. This is one area in which the United States hopes to improve nuclear security by improving operators' capability to measure plutonium from reactors.

Browne then discussed how to align the interface between physical protection systems and nuclear material accountancy systems. It may be obvious that the nuclear material accountancy and physical protection system should be integrated in order to effectively promote the protection of the material. But in particular, it is important that the physical protection zones and the nuclear material balance areas overlap. If the material balance area is spread between two physical protection zones or vice versa, the ability to effectively respond to

an incident is reduced. It is best to ensure that there is consistency between these areas.

There is certainly a need to exchange information between the nuclear material accountancy and physical protection systems. Access to facilities is controlled by physical protection. But those responsible for physical protection also need to have intrinsic information about the material that is being protected there: What are the types of emissions? What are the dose rates? An example would be that the physical protection system should know what is required to move a particular source. Is a crane required? How much shielding would be required? Where is that shielding located? Sharing of this type of information enhances security.

In the interface between the nuclear material accountancy and physical protection systems, the nuclear material accountancy is designed to detect the material removal and the physical protection system is designed to prevent that removal. The security function relies on the same accounting systems used for bookkeeping. Then on the physical protection side, there is everything from the vulnerability assessment to the concept of operations regarding how to respond to actual removal. But there is a fair amount of overlap in between, in the form of the material balance area and the characteristic information.

Knowledge and information or data from both operations and the health/safety aspects are important for both accountancy and physical protection systems, and for overall nuclear security. Operations and occupational health and safety are additional pieces of information that help provide confidence in a security system. On the operations side, consider the question: Is a crane movement required for this particular process? If it is, then when that process is observed, one can be more confident. But if it is not needed and one sees the crane moving, then either from the physical protection side or the nuclear material accountancy side, further scrutiny is warranted.

With regard to health and safety, most facilities have contamination monitors. That information can be incorporated as well to provide an indication of abnormal conditions and potential theft.

Browne concluded his remarks with the following highlights:

- Nuclear security relies on a well-developed, integrated combination of nuclear material accountancy and physical protection.
- A risk-based approach is best to ensure that the fidelity is right. The nuclear material accountancy system for a CANDU facility is not necessarily the right match for a fast reactor.
- There are supplemental measures that can be incorporated to give increased confidence in a security system.
- Ultimately, the goal is to protect the public. This is a twofold measure. One is to ensure that the misuse of material or sabotage of a facility is prevented. But almost as important is to instill confidence in the public that the people at the facility are good stewards of the nuclear material.

Nuclear Materials Security at Non-Reactor Civilian Facilities

Indian Perspective

A.R. Sundararajan began his remarks by outlining the components of an effective control system for ensuring safety and security of radioactive sources. Via these components, the AERB ensures: an inventory of sources in the country, document control (monitoring the status of sources), regulatory inspections, secured sources at various stages of management, training of concerned public officials, and an Emergency Management System. Thus far, there have been no reports of major security incidents of nuclear material diversion from fuel cycle facilities involving individuals or groups of a criminal nature. However, complacency has to be avoided due to the potential significant consequences of a radiological event, and to maintain public confidence in the development of nuclear energy.

India has chosen to develop a closed fuel cycle because of its limited domestic sources of uranium. The closed fuel cycle allows for resource extension and sustainability, waste classification and isolation, a reduction in demand for repository space, and proliferation resistance (no plutonium mines leading to a reduced threat for future generations).

As part of the closed fuel cycle, India began its Fast Breeder Reactor (FBR) program with the construction of the Fast Breeder Test Reactor (FBTR), a 40 MWt (13.5 MWe) loop type reactor. The FBTR has been in operation since 1985. The Mark-I fuel has achieved a burn-up rate of 155 GWd/t at a maximum linear heat rate of 400 W/cm without clad failure. It has an expanded hybrid core of mixed carbide and high plutonium mixed-oxide fuel (MOX): 20 percent of the core has 44 percent plutonium MOX. There is an experimental Prototype Fast Breeder Reactor (PFBR) MOX fuel assembly at the centre of the FBTR.[1]

The 500 MWe PFBR was designed and constructed indigenously. Beyond the PFBR, India plans to build six commercial units of 500 MWe FBR (twin unit concept) similar to the PFBR with improved economy and safety by 2020. Subsequent reactors will be 1000 MWe units with metallic fuel, and the first unit is expected by 2027.

Sundararajan stated that there are certain proliferation resistant features of the fast reactor fuel cycle, which include modification of the plutonium uranium extraction (PUREX) flow sheet for co-processing of uranium and plutonium, higher contents of plutonium-240 and higher actinides, and the development of pyrochemical reprocessing for spent metallic fuels from future FBRs. The Indian fuel cycle strategy envisions using the minimum cooling period for fast reactor fuel and consequently the minimum out-of-pile inventory of plutonium. A versatile hot cell facility for testing the reprocessing process flow sheets and prototype equipment was commissioned in December 2003. After 2003, the

[1]MWt = megawatts thermal; MWe = megawatts electric; GWd/t = gigwatt-days per ton of initial heavy metal; W/cm = watts per centimeter along the fuel rods.

facility has processed FBTR plutonium-carbide fuel rods with burn up of more than 150 GWd/t with a cooling period of about two years and fission products with specific activity of about 700 curies per kilogram.

Bulk processing of plutonium from fast reactor fuel especially in concentrated form provides great potential for covert diversion by skilled adversaries. High burn up plutonium, particularly from fast reactors with large contents of plutonium-240 and higher actinides is not attractive for nuclear weapons, but stolen plutonium in view of its high toxicity and scare value can however be used in a radiological dispersal device (a dirty bomb).

To minimize the vulnerability of nuclear material, an integrated fuel cycle management system has been adopted. This includes minimizing the storage time of processed plutonium, minimizing the transportation of separated plutonium, and converting plutonium into MOX fuel. In fast reactor facilities, the vulnerability of the nuclear material increases vastly as the process moves from the front end of the cycle to the final product purification. The complexity of mechanical and chemical steps at the front end, due to high radioactivity requiring shielding and remote handling, acts as a great deterrent.

Nuclear safety and security serve a common purpose: protection of the worker, the public, and the environment from a large release of radioactive material. There is a growing recognition that it is prudent to have an all-hazards approach to national security that addresses a range of threats from natural disasters to man-made accidents or malicious attacks. There is one agency to oversee safety and security. Many of the principles of protection for safety and security are common, although the implementation may differ. Both objectives are pursued using a defense-in-depth approach through a number of redundant, diverse, and independent controls to reduce the likelihood of faults from occurring, to detect and control them when they occur, and to mitigate the consequences should the controls fail. The synergies between the requirements for these areas should be identified and any conflicts resolved.

Protection in depth requires an adversary to bypass or defeat a number of protective measures in sequence to attain a goal. These protective measures include physical security systems, administrative controls, and accountability. Some measures can serve safety and security functions simultaneously such as the massive shielding structure. Some measures may cause conflicts because of safety and security requirements. For example, the security requirement that the number of access points be kept to a minimum in a plutonium handling area can conflict with the safety requirement to have enough emergency exits to get out of the plant areas quickly in the event of a criticality accident. Likewise, security vulnerabilities could be created during an accident. Therefore, an objective optimization process is needed to support an integrated risk management plan. This has to be carried out at all stages of the plant from siting, design, to construction and operation. Site selection and design should take into account physical protection needs as early as possible and address the interface between physical protection, safety, and nuclear material accounting to avoid any conflicts and to ensure synergy among the three elements.

All plutonium facilities are subject to strict nuclear material accounting systems and physical protection measures. These include, protection in depth with multiple layers of protection, portal monitors sensitive to neutrons and gamma rays, containment and surveillance systems together with NMA provide a measure of confidence that potential diversion paths are not being used for clandestine purposes by criminal elements.

In plutonium reconversion/fabrication facilities where vulnerability is relatively high, near real time accountancy can be applied to improve the detection sensitivity for loss or diversion of plutonium. Concerted efforts are taken to include design, operation and control features aimed at reducing material unaccounted for and also to incorporate better plutonium measurement techniques.

The diversion of nuclear material from facilities can also be minimized by automating the process. Through automation, access to the nuclear material can be minimized and the number of operators can be reduced, thus reducing the possibility of theft or diversion. The International Commission on Radiological Protection (ICRP) recently reduced the exposure limit to the eye from 150 mSv to 20 mSv. To reduce the individual exposure in plutonium fuel fabrication areas, one has to deploy more people, which may conflict with security requirements to keep the staff at a minimum. Therefore, the need for automation of the fabrication process is driven both by security and safety requirements.

Remaining challenges to the security of a fuel cycle facility include: the need for automation of the process operations and material accounting, new vulnerabilities from increased use of computers, cyber attacks on computer systems used for process control, nuclear material accounting, and physical protection systems. The absence of structured guidance documents on security similar to the safety codes and guides is also a challenge. Currently, no hierarchical documents exist for security and there are concerns about inadvertent revealing of plant security vulnerabilities. Consequence analysis is essential and conducted using a design basis accident and a design basis threat. A primary distinction is that nuclear safety regulation is not prescriptive, whereas nuclear security regulation is prescriptive.

Finally, Sundararajan concluded that the lack of sharing of experiences from fuel cycle facilities in other countries remains a challenge. Likewise, there is a lack of standardization across facilities, which makes security difficult as well. He said that India has excellent probabilistic safety assessment models for safety assessment of nuclear facilities but does not have vulnerability assessment models for security assessment of nuclear facilities. The organization of appropriate training programs to promote security culture would be beneficial.

U.S. Perspective

Michael O'Brien began his presentation by stating that the protection of nuclear facilities has evolved over many decades. This evolution has been

necessitated by advances in technologies as well as the need to adapt to a chang-changing threat. According to the IAEA Guide INFCIRC 225 Rev.5,[2] which a vast number of nuclear facilities world-wide use as their principle guidance, nuclear facility physical protection should be based on a defined threat. This threat and the characteristics of the threat are defined at the government level in the United States. The facility physical protection system would be expected to adequately address sabotage and theft attempts by adversaries defined in threat guidance and therefore requires development of appropriate protection strategies and proper implementation.

When determining the threat, O'Brien stated that the threat guidance, generally referred to as a design basis threat DBT, describes the number and attributes of adversaries. A common DBT would define a group of outsider adversaries and one or more insider adversaries, and outsider adversaries colluding with an insider. The capabilities of the adversaries would also be defined in terms of their knowledge, skills, weaponry, and equipment.

The philosophy of protection in the United States includes the notion that nuclear facilities should be designed to allow for redundancy and defense in depth in the protection system to avoid single point failures and to force adversaries to defeat several protection elements in order to achieve their intended task. The facility layout may also be designed in a way to afford a layered or graded protection approach in which protection measures increase closer to target locations.

A protection system may encompass several principle objectives. These may include protection against: theft by outsider and/or insider adversaries, sabotage by outsider and/or insider adversaries, or cyber attacks. The combination of protection systems and protective force deployment must effectively mitigate each of these threats. This deployment may require the implementation of multiple strategies.

The protection strategies, containment, and denial, are specific to the type of threat one is protecting against. A containment strategy is used for protection against theft of nuclear material, through the use of appropriate detection, delay, assessment, and response capabilities. Protective force assets must be able to respond in time to interdict, contain, and neutralize an outsider adversary force before completion of an attempted theft. A denial strategy is used for protection against sabotage of nuclear material, through use of appropriate detection, delay, assessment and response capabilities. Protective force assets must be able to respond in time to interdict and neutralize an outsider adversary force prior to the adversary forces arrival at the target location thus denying their access to the location and their sabotage attempt.

[2]Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA Nuclear Security Series No. 13. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.

Strategies against an insider threat encompass some appropriate combination of separation of duties, limited access, limited responsibilities, compartmentalization, two-person rule procedures, material surveillance, material controls and accountancy measures, as well as safety procedures and systems in order to increase the likelihood of detecting an insider attempt of theft or sabotage. A human reliability program may be administered to further enhance an insider protection program.

A strategy against a cyber threat encompasses analysis of electronic networks and the identification of appropriate electronic measures to detect network penetration attempts.

According to O'Brien, a strong physical protection system (PPS) design effectively integrates people, procedures and equipment to meet the objectives of the system. The protection system design must facilitate protection elements working together to assure protection rather than treating each single element separately. For example, to be effective, the manager should ensure that fences, sensors, delay systems, closed circuit television assessment systems, procedures, communication systems, and protective force personnel act as an integrated system meeting protection objectives. The primary PPS functions are to detect, delay, assess, and respond to adversary actions.

Intrusion detection may consist of an array of technologies designed to detect penetration by an adversary. Some examples include: exterior/interior sensor technologies such as microwave, active or passive infrared, vibration, magnetic field, and electric field. Delay systems decrease the adversary rate of progress toward the target allowing an adequate number of protective force personnel to respond in time to stop a malevolent act. Some examples include: fences, walls, doors, structural enhancements, vehicle barriers, smoke or fog visual obscurants, entanglement systems. Assessment systems aid in the visual verification of detected adversary actions, as well as aid the protective force in the subsequent engagement with the adversaries. Some examples include: closed circuit television cameras, lighting systems, and posted or patrolling protective force personnel.

Protective force personnel provide the response actions to interdict and neutralize adversaries. The response force is generally composed of tactically-trained primary responders, tactically-trained secondary responders, and posted or patrolling protective force personnel who augment the engagement by primary and secondary responders.

To achieve an appropriate level of system effectiveness, O'Brien noted, the entire protection system must operate in a complementary and integrated manner. Protection elements do not have to be physically integrated, but rather have to work in synergy to achieve the overall protection objective. Three noteworthy points of integration include:

(1) nuclear material controls, which allow material accountancy and physical protection to work in a complimentary fashion

(2) protection systems and protective force, which form the main core of the protection system
(3) command and control system integrating physical protection systems as a single command center operated by a protective force.

Nuclear material controls may include: material surveillance systems, point sensors, vault-alarm sensors, two-person procedures, material tie-downs, and entry control measures such as nuclear detection portal monitors, metal detectors, and electronic access controls.

Physical protection systems provide the means for the protective force to detect, delay, and assess adversary actions allowing the response force to tactically engage the adversaries in a timely manner. When needed in situations of shortcomings, compensatory measures for an integrated system can be either physical protection system elements or protective force personnel. Integration of physical protection systems into a single alarm control and display unit with assessment, entry control, and communication capability provides protective force personnel the ability to effectively operate the entire system for daily operations and in emergency situations such as adversary malevolent acts.

Protection systems should be in a constant state of evaluation. System effectiveness should be validated and any shortcomings addressed in a timely manner. This is often best implemented through a performance assurance program, which is a means to collect and store system data in a single location for use by analysts in verifying system effectiveness. A system testing plan should define the manner and frequency system components are tested for functionality as well as performance against design criteria.

O'Brien said that all critical systems and their critical elements should be performance tested regularly. Tests can be at the system level or component level. Test results should be documented and archived for use by system administrators, performance assurance program administrators and vulnerability analysts.

Protective force personnel should be subject to periodic testing to validate tactics, procedural compliance, and response times. Test results should be documented and archived for use by performance assurance program administrators and vulnerability analysts. Similarly, material control and accounting (MC&A) systems and their critical elements should be performance tested regularly. Tests can be at the system level or component level. Test results should be documented and archived for use by system administrators, performance assurance program administrators and vulnerability analysts. Vulnerability analyses and the documented system effectiveness level should be validated on an annual basis and when a change in operations or facility configuration occurs.

In summary, nuclear facilities require the highest level of security due to the high consequence to the public if a malevolent act were to occur. Proper protection planning, design, and implementation approaches are well documented and shared within the global security community.

Safety, Security, and Safeguards

Paul Nelson began by stating that his presentation would emphasize nuclear security, but that he also would refer to safety and safeguards as well. Together they make up what is known as the "3 S's." He also focused on the educational aspects of all three, especially security and research.

As has been stated by other presenters, public perception of safety and security is essential, especially in a democracy where public confidence is crucial to nuclear activities. For purposes of nuclear security, it is important to reassure the public that appropriate measures are being undertaken, while not revealing information that might be useful to any potential adversary. In the United States, the responsibility for security of civil materials resides with the (typically private) entity owning the material.

Nelson then provided an overview of the Texas A&M University's Department of Nuclear Engineering at which graduate students do scientific and technical work with policy overtones. Other U.S. universities with similar programs in nuclear security include the University of California at Berkeley, the University of Missouri, the University of New Mexico, and the University of Tennessee. Nelson noted examples of possible research projects for Indo-U.S. collaborative efforts that could be conducted either through these universities or elsewhere.

He provided examples rooted in the so-called "risk equation." Figure 2-1 defines risk as the expected value per unit time of the consequences of an adverse action. At that level of generality, the concept of risk is equally applicable to safety, security, and safeguards, and in fact probably has been most extensively applied to safety in the form of so-called risk-informed approaches to nuclear safety issues. The objective of the defending force is to minimize risk, but Nelson stated that probability and consequences should not be overlooked.

The problem of how to assess quantitatively the probability (frequency) of attack in the security and safeguards areas may be one possible joint research project. This could, if successful, move security toward the risk-based approach to safety. The currently accepted alternative is to design safety measures to the design basis threat DBT.

Risk = $P_A P_S C$,
P_A = Probability, per unit time,
that an attack occurs;
P_S = Probability an attack is successful,
given that one occurs;
C = Consequences of a successful attack.

FIGURE 2-1 The so-called "risk equation" defines risk as the expected value per unit time of the consequences of an adverse action. SOURCE: Nelson, 2012.

A second research opportunity could be directed toward affecting some commonality in the measure of consequences across safety, security, and safeguards. The challenge is difficult, because consequences are not measured in the same terms (e.g., property damage vs. lives lost). Even within a single one of the "Ss"—for example safety—there are strongly held opinions regarding rational evaluations, and these differences are further confounded by lack of some basic knowledge such as the linear no-threshold hypothesis for very low radiation doses.

The third possible opportunity for collaborative research Nelson proposed lies in the area of information security. It is based on the observation that at many nuclear installations there is need for communication resources for purposes of both security and safeguards. It is therefore an obvious idea to achieve economies and efficiencies by sharing resources between these two needs. The problem of course is how to ensure integrity of the two data streams, especially given that for security the host nation is the protectorate, while for safeguards it is the presumed adversary. The research question very roughly could be how to use software-based methodologies to achieve that integrity.

The fourth and final example of a possible research collaboration is on consequence management training tools, such as the development of a plume simulator for handheld instruments, or even smartphone applications.

Nelson also noted that there could be a junior-level exchange program between Indian and U.S. students to jointly address these and other issues. From his perspective, an ideal arrangement would be an "experiment" in which a few U.S. graduate students in nuclear engineering, for example, could carry out research internships at appropriate Homi Bhabha National Institute (HBNI) campuses in the summer of 2013, to be followed by similar research-oriented visits by current HBNI students or recent graduates later in the fall of 2013. They could be matched-up in pairs to permit six months of continuous effort by the same people in the same problem area. The hope is that these exchanges would lead to substantial results. He noted that there are some universities in the United States interested in this idea. Hopefully there would also be Indian universities interested in hosting students from the United States as well.

DISCUSSION

The initial question was about personnel reliability programs and who, in the United States, has access to sensitive target areas. For example, would guards have access to sensitive areas, because this might constitute a type of insider threat if the person were to be ideologically inclined. There were three attacks on military targets, not civilian, likely due to insider threats.

O'Brien replied, that, yes, the personnel reliability program does apply to the guard forces. He noted that because their duties or responsibilities relate to the protection of the material, the majority of the MC&A personnel, material handlers in various functions at work that environment, will be under the

program. Protective force personnel are under the program. People who main-maintain the systems are under the program, and even some of the first-level supervision of those personnel. The main group of those who either have direct access or who could obtain access to the material are covered by the program in the United States.

Kumar replied that to the best of his knowledge, India uses the same approach. Anyone who could potentially be an insider threat, including the top manager, is covered by the program. This is always taken into account in the design phase as well. Other measures are also taken. He continued by stating that when new guard forces enter the system, or come to a new facility, a check is performed; there are always checks and balances.

A participant continued, in many of India's security facilities, there is a layer of overall security, then there is the Central Industrial Security Force (CISF). There is separate training for CISF personnel involved in specific duties at some of facilities. These guards know that if they are assigned to a BARC facility, they have to have additional training. However, what is actually going on inside is something that they may not know at all. Access is granted on "a need-to-know basis." They do have to be sensitized with additional information. They are also monitored. Also, the CISF forces are rotated perhaps as often as every one or two months.

A question was raised about security at nuclear facilities from the front end to the back end. Last year an IAEA Scientific Committee studied the effects of atomic radiation for a 20-year period, 1987 to 2007, and there were only three accidents. There were no deaths or injuries related to the absence of nuclear security. In fact, the IAEA safeguards group, to which safeguards accounting reports are sent every year for all members of the NPT with the exception of the nuclear weapon states, stated that all Indian facilities have nuclear security under control. There has been no diversion, which under IAEA Guidelines means that the probability of diversion of more than 1/3 of standard quantity is less than 1/3. So as far as the nuclear material at nuclear facilities are concerned, there is no guarantee that nothing will happen in the future but thus far there has not been any material breach of security.

On the other hand, the same IAEA scientific community said that orphan sources are a breach of nuclear security, and over the 20-year period from 1987 to 2007, 16 deaths have taken place, and there were 28 earlier incidents with more than 200 deaths, which means that the breach of nuclear security in the case of radiological material is far more serious than anything that has been contemplated in the nuclear facilities, and, of course orphan sources means they come only from industrial or medical applications. Those accidents are different. These orphan sources mean a breach of nuclear security, however, this was not discussed at the workshop. Is the real consequence of a breach of security for nuclear radiological materials far more serious and how do we adjust that? What are the concerns in coming years? There must be orphan sources in the United States as well as in India because there has not been a comprehensive check. There have been a few instances where Intercel radiography cameras

have been lost or nuclear gauges have been procured and not used lying idle for quite a long time. Some more attention should be paid to these sources. It is a public concern and serious, and in the case of Brazil, far more people were affected by unintentional radiation exposure from a radiological source in Goiania than anything that has happened in any other place. The offsite impact of Goiania is far more than the offsite impact of any nuclear accident at Chernobyl and recently Fukushima.

A participant noted that the Goiania incident was not a malevolent attack. In other words, incidents regarding orphan sources often arise out of ignorance. People who handled the materials did not know what the consequences would be, including the Mayapuri incident. After the Mayapuri incident, a system has been put in place in India to inventory all of the radiation sources and there is an exhaustive computerized database system. Today, with this particularly high category source, nearly 100 percent of the material has been inventoried. With lower category sources like that used in diagnostic radiology, the inventories are still to be completed because there is a very large number of sources dispatched. A large number of people have been trained in the last two years, as many as 2,000, in hospitals, in port authorities, in customs services, clearing agents; and all of these people have been sensitized with respect to the risk associated with this kind of source.[3]

Suppose a person receives a source from abroad, at the end of its useful life, it would not be exported. Ten years ago, there were no stipulations in India to address such incidents. Today, no one can import a source from abroad unless there is a commitment by the supplier to take the source back after its useful life in the country. The rules have been tightened and enforcement has been tightened. It is impossible to get a source imported without the clearance of AERB, and clearance for import, for use, for the operation, and for decommissioning and repatriation, without a license at every stage from the regulatory board.

Another workshop participant expressed surprise that a nuclear security breach includes an accident or a malevolent attack by a terrorist or a demonstrator. There is no distinction between an intentional or an unintentional act. Both are considered a breach. Second, in a 20 year period, 42 people died. For those 42 people, it makes no difference whether there was a breach of nuclear security because of a malevolent attack or a terrorist attack. Third, yes, these materials were handled, but they were handled not knowing what they were. Non-malevolent acts may also lead to complacency.

A participant from the United States added that in the early 1990s, requirements were added to conduct vulnerability analyses on special nuclear material, including what was defined as radiologically toxic material located at a

[3]Comptroller and Auditor General of India, Activities of Atomic Energy Regulatory Board, ReportNo. 9 of 2012-13. Available at http://saiindia.gov.in/english/home/Our_Products/Audit_report/Government_Wise/union_audit/recent_reports/union_performance/2012_2013/SD/Report_9/Chap_6.pdf. Accessed September 3, 2013.

site. Owners now have to analyze vulnerabilities, the risks associated with those items, and define security for those items, as well. And that has been going on ever since the early 1990s at Department of Energy (DOE) sites.

Another participant added that the problem seems to stem more from in-industrial radiography sources because a licensed person may wish to buy a source, but then pass it on illegally to someone else. What if it is lost? There was even a case some years ago when a disgruntled employee stole a source and threw it into a public body of water, and then it had to be retrieved. These sud-sudden cases are far more difficult to resolve, but they need to be addressed in whatever way possible. There will always be some situations that cannot be ad-addressed.

The issue of retrofitting was then raised. How does this work? Architects are now giving us the option of greening older buildings for energy conservation with green technologies. How do you actually apply this design to an older building to make it secure and explain this to the budgetary authorities?

Another participant replied that this is a very good question because often these concepts and methodologies are presented as if we are dealing with perfect facilities, and in reality, no facility is perfect. The truest answer is that we do analysis, assess the risk, and sometimes we will end up with targets that are too close to perimeters or any number of issues. One just really has to do the best one can until the point is reached where one feels an adequate risk level has been achieved, and sometimes additional compensatory measures are unavoidable. All of this is driven by the scenarios analyzed at a particular facility. All facilities are different, of course. Whether you have done an adequate job or not is the end result of the risk equation. If that is not achievable, then the true measure is consolidation of material, movement of the material to other locations, and that happens as well.

A participant asked a follow-up question about whether or not decisions are made on a budgetary basis. Is a facility then declared as a high risk area? In reply, if the retrofit really truly cannot be done for whatever reason, the material is removed. In the United States, high-risk situations are not tolerated. The mission is moved elsewhere or that activity at that particular location is stopped.

Another participant added that sometimes regulations are prescriptive and not performance-based. An example would have been the requirement to have a Perimeter Intrusion Detection and Assessment System (PIDAS) around certain types of facilities. At the Savannah River Site, funding was requested to put the PIDAS around the separations facilities, but it just was not going to happen. There was not enough money in the budget. So, the risk was analyzed, and in that particular situation, it was judged that it was not necessary for the task being performed. The appropriate risk level could be achieved without funding that type of upgrade. So that would be an example where budget came into play, and the problem was reviewed and the decision was not to do the upgrade because it just didn't make financial and security-base sense.

Raymond Jeanloz asked about avoiding a conflict of interest in that par-particular case. Were there outside reviewers, an independent audit or something

like that? Exceptions should be allowed without opening the door to conflicts of interest. In response, the participant replied that to the best of his memory, there was a congressional line item to do that upgrade, and the cost grew too large, so there was an independent analysis conducted.

Another participant recalled the earlier discussion about how the design basis threat DBT can drive costs up and down. There was an experience in the early 1990's when a local DOE office asked to use the vulnerability analysis results, to conduct sensitivity analysis by adding and taking things away. They requested that certain items be eliminated, basically stripping the protection to determine how much money could be saved by taking protection away, and the facility was forced to do this. That was prior to the events of September 11, 2001. Subsequently, the DBT went up, and the facility was less equipped to ramp up to appropriate levels of security, and it cost quite a bit of additional money to have the right level of security. Therefore, as a note of caution, do not use the vulnerability analysis results as a kind of a cost metric. It is really a performance metric of the system, but it can also be misused, if the results are used the wrong way.

V. Venugopal agreed that previously, many of the radiological sources were not really properly accounted for, but now the bulk of radiation sources are more secure: sources associated with isotope technology are secured, databases have been completed, and frequent visits to the sites are made to see that everything is in place. This is one of the major issues with respect to radioisotopes in the public domain. It is a double edged sword. For example, Am241 were extensively used in various places as smoke detectors. And in the United States, 10 years earlier, a school student had collected large number of sources and material was dispersed in that area. His house was contaminated. The area was contaminated. So much money was spent. Now, this source was removed from smoke detectors. BARC has collected all of these smoke detectors and disposed of them after installing the new varieties. So these are the problems.

This is obviously a serious concern. At DOE, there are two programs dealing with this issue. One of them is well logging in the oil industry where radiological sources have been used and still are being used in reasonably large amounts. DOE is investing money to find an alternative to americium and beryllium sources and trying to see if one can receive neutron radiography not using radiological sources. The Department of Atomic Energy would certainly explore similar things. And the second one is DOE's program, offsite sources recovery program. It is not about orphan sources, but rather an offsite sources recovery program by DOE and Los Alamos National Laboratory. They help remove some of orphan sources and secure them. There is a lot that can be done.

Communication also needs to happen because one can never completely avoid risk. It would be difficult to go to a drilling company and ask them to have all of their security measures consistent with those of nuclear and radiological facilities. How do we educate them? How do we procure orphan sources? Some of this is still being thought through.

Of these very technical issues, a participant stated that his source of concern is nuclear terrorism. During the Washington and Seoul Summits the Indian government and 40 other governments have committed at the highest level to nuclear security. So if one is concerned with nuclear terrorism, then one is concerned with security of materials of all forms, i.e. plutonium and uranium in the different forms, and irradiated fuel, and also radiological sources. Frankly, if there is a nuclear terrorist attack, we do not care what kind of material is used, the speaker said. The implications of a terrorist act with radioactive material is very serious. It is difficult to address because the sources are widely dispersed, which could increase the threat of an improvised explosive device. Is there currently a procedure in India to check every site of a bomb explosion for radioactivity, because without ever knowing it, there may have been radioactive material mixed with chemical explosives, only to be discovered much later. People who were exposed may have moved away. Maybe every chemical bomb explosion anywhere should also be checked for the presence of radioactivity.

3

Physical Security at Civilian Nuclear Facilities

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- Nuclear security has three distinct steps: (1) define the requirements, (2) design the physical protection system based on the requirements, and (3) evaluate the physical protection system to assess whether it meets the performance requirements.
- The most difficult adversaries to address using the physical protection system are terrorists, but activists and demonstrators are also difficult because of the ambiguity of their actions and intentions.
- The insider threat is a worldwide concern for nuclear security because an adversary with a colluding insider is very dangerous.
- The vulnerability assessment process can be divided into three broad phases: characterization (target identifications); analysis (identifying vulnerabilities); and neutralization and system effectiveness.

Promising Topics for Collaboration Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions are not those representing the consensus of the participants, but are rather a selection of those topics offered by individual participants throughout the presentations and discussions.

- To address the growing demand and diverse technology requirements, standardization may be an area for joint discussion because it is essential for benchmarking and for cost-effective systems.

- Potential saboteurs can utilize a protest by mixing with activists and demonstrators who could gain entry. Understanding how to address materials security in these scenarios is an area of potential discussion for U.S. and Indian experts.

Technologies and Physical Security of Nuclear Materials: An Indian Perspective

Ranajit Kumar described technologies for physical security of nuclear material (see Table 3-1). He began by noting that India's commitment to security of nuclear material comes from the highest levels of the government, illustrated by the statement made by Prime Minister Manmohan Singh explaining that the Indian Atomic Energy Act[1] provides the legal framework for securing nuclear materials and facilities and committing India to developing a Global Centre for Nuclear Energy Partnership, one element of which will be a school for nuclear materials security. In addition, India is a party to the Convention on the Physical Protection of Nuclear Material and its 2005 amendments.[2]

The major concern about nuclear material primarily derives from the fact that it can be used to make nuclear explosive devices, which can be highly catastrophic. Nuclear sabotage, a major concern for nuclear facilities like nuclear power plants, can also be catastrophic. A dirty bomb or radiological dispersal device is not a weapon of mass destruction, but a weapon of "mass disruption." Nuclear security has five key components, according to the Nuclear Threat Initiative: quantity and sites, security and control measures, global norms, domestic compliance

TABLE 3-1 Potential targets worldwide that require nuclear security. Compiled by Kumar from International Atomic Energy Agency data.

Number of items	Type of Item
25000	nuclear weapons
3000	tons civil and military HEU and Pu
480	research reactors (>160 with HEU)
100	fuel cycle facilities
440	operating nuclear power plants
100000	Cat I and II radioactive sources
1000000	Cat III radioactive sources

[1]The Department of Atomic Energy, The Atomic Energy Act, 1962. Available at http://dae.nic.in/?q=node/153. Accessed September 3, 2013.

[2]IAEA. 1980. Convention on the Physical Protection of Nuclear Materials. Available at: http://www.iaea.org/Publications/Documents/Conventions/cppnm.html. Accessed September 20, 2013.

and capacity, and societal factors.[3] Kumar focused on security and control measures noting that nuclear security is more than gates, guns, and guards.

Nuclear security has three distinct steps: define the requirements, design the physical protection system based on the requirements, and evaluate the physical protection system to assess whether it meets the performance requirements (see Figure 3-1). The third step feeds back into the second step so that if the system does not meet the end objective of neutralizing the adversary with a certain probability, the physical protection system can be adjusted or redesigned.

The first step is to define the requirements of the physical protection system. This step includes characterizing the facility, identifying the targets that need to be protected, and defining the threat the system must protect against. A graded approach is taken in target identification. The International Atomic Energy Agency (IAEA) has categorized nuclear material (Category I through III; see IAEA Information Circular 225/Rev 5)[4] according to handling requirements. For unirradiated

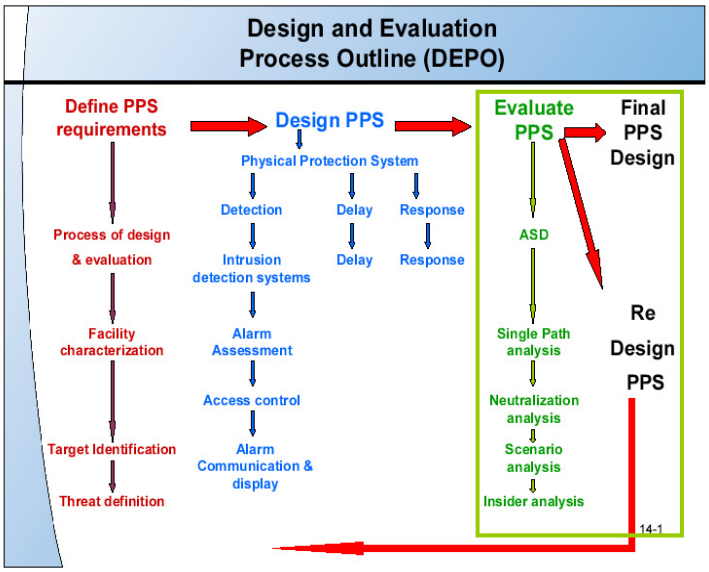

FIGURE 3-1 Diagram of the design and evaluation process outline (DEPO). SOURCE: Kumar, 2012.

[3]Choubey, Deepti, Sam Nunn, Joan Rohlfing, Page Stoutland. 2012. NTI Nuclear Materials Security Index: Building a Framework for Assurance, Accountability and Action. Available at: http://www.nti.org/analysis/reports/nti-nuclear-materials-security-index/. Accessed September 3, 2013.

[4]Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA Nuclear Security Series No. 13. Available at: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf. Accessed September 3, 2013.

material, the category is based on the hazard of the material or its perceived value to a malefactor, which in turn is based on its utility in making a nuclear explosive and the quantity that is present. For example, unirradiated plutonium in quantities of 2 kg or more qualify as Category I. Most nuclear power plants use Category III nuclear material, except for some research reactors.

There are several considerations in defining the threats that the system must protect against. The threats may include thieves, saboteurs, terrorists or protesters. For any adversary, the requirements include how many people are involved; whether it involves outsiders, insiders, or a combination of the two; the motivation (ideological, economic benefit, or something else), and; objective or intention (e.g., are they interested in sabotaging a plant to disrupt the power plant, to disrupt the power production, or is their intention to take the nuclear material?). The threat definition also includes the adversary's tactics (force, deceit or stealth) and capabilities (numbers, training, knowledge, weapons, equipment). The various aspects of the threat are summarized in the form of what is called the design-basis threat (DBT). India has a national DBT for the design of physical protection systems for all civilian nuclear power applications and civilian nuclear facilities. The DBT is confidential for obvious reasons.

Kumar said that his initial perception was that the most difficult adversary to address using the physical protection system would be terrorists, but he understands now that even activists and demonstrators are difficult because of the ambiguity of their actions and intentions. That said, the insider threat is a worldwide concern for nuclear security because an adversary with a colluding insider is very dangerous. They can be internally motivated or externally coerced, passive or active, and nonviolent or violent.

After defining the requirements comes the design phase. Based on the national DBT, a local and facility-specific threat document is prepared because there are certain threat elements that are specific to a particular locality, a particular region, or a particular state. All facilities are required to prepare their facility-specific DBT document and the physical protection system is designed to that threat.

There are three elements of the physical protection system: detection, delay, and response. Detection can be carried out by intrusion sensing (exterior and interior) and by entry control and other methods. Typical sensors include infrared thermal cameras with video analytics. Another tool is to look for objects that are not permitted—for example, explosives—to detect threats to the facility. Entry control is used for the purpose of allowing authorized personnel to gain access to the facility to carry out their normal duties and requires both identity validation and access control.

The target should be protected in such a way that the system provides a certain minimum delay to the adversaries to reach, gain access to, and either sabotage or take the target. In theft scenarios, the facility protectors have both the time to reach the target and the time it takes the adversary to leave the facility. The delay elements are walls, structures, barriers, including active barriers or dispensable barriers (e.g., slippery or sticky foams). For delay to be effective,

the protection system should detect an adversary action as early as possible and notify the response teams.

The Central Industrial Security Force (CISF) under the Ministry of Home Affairs is the primary response force for nuclear facilities in India. They have a separate set of training requirements and weapon qualifications for guarding nuclear facilities. Depending on the requirements, the local police and some of the national response forces also may be called upon.

Kumar noted that most of the technologies that are deployed in Indian nuclear installations for nuclear material security, as well as for nuclear facility security, are developed in-house by either the Bhabha Atomic Research Centre (BARC) or Electronics Corporation of India, Limited. They are designed to particular specifications because of the need for reliability given that some elements can compromise the security of a nuclear installation if they do not function properly.

BARC has also designed security systems for non-nuclear facilities, applying the systems engineering approach used for nuclear facilities to other installations. For example, BARC designed security for the Indian Parliament and some of the same design principles, such as for vehicle barriers, were taken from nuclear facilities.

Nuclear material control and accounting is another major component of nuclear material security. This system is the first to detect whether there is any diversion of nuclear material occurring. The Indian Department of Atomic Energy has the nuclear material accounting group, which is responsible for carrying out the nuclear material and accounting.

In the inner layer where the nuclear material is stored, some of the physical protection techniques, such as the two-man rule to open locks, are applied. Similarly, there are several electronic locks designed indigenously that are used. Material is guarded by using indigenously developed electronic seals for storage containers and portals for detection of nuclear material in personnel monitoring. Kumar noted that BARC has also developed other radiation detectors primarily for border applications (i.e., to detect illicit trafficking), and handheld detectors for searches. The government of India mandated that the portals be installed across all of India's airports and seaports. So far, they are deployed in a couple of seaports.

The moment one utilizes any network-based system, it is vulnerable to an attack from external sources and they can gain access. That is why information security is an integral part of the program (see Figure 3-2). India has developed a secure messaging and voice communication device that sits within a mobile device and helps communicate in a secure manner, both for messaging and voice communication.

India has requirements for both safety and security of nuclear material transport. India does real-time tracking of secure vehicle transportation using its geostationary satellite. The system also utilizes the local Global System for Mobile Communications or Code Division Multiple Access (CDMA) mobile communication network. They are completely tracked within India from a central monitoring station.

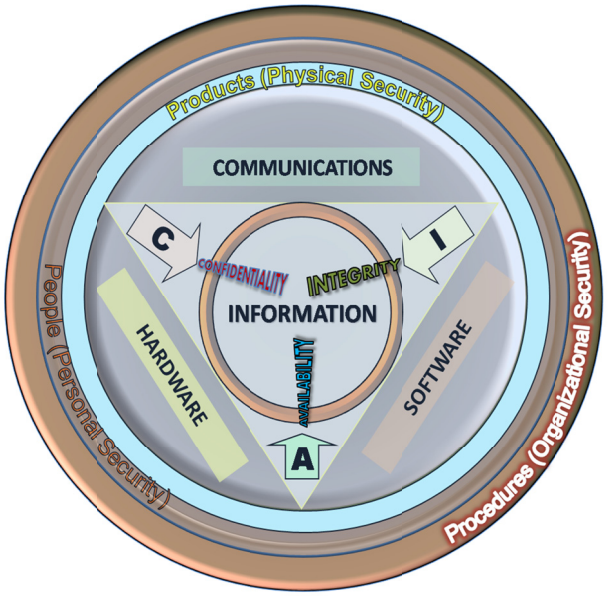

FIGURE 3-2 Conceptual diagram of the elements and interconnections of information security. SOURCE: Kumar, 2012.

Finally, Kumar said, all of these elements are combined in an integrated physical protection system (PPS). An integrated PPS is in place at all nuclear installations and is a prerequisite for new builds. The requirement is to address nuclear security using the right mix of security hardware, procedures, and properly trained personnel. One without the other makes the system incomplete. Further, the systems cannot be kept in isolation; they have to interact with each other. But they must be kept secure, particularly when the whole system is becoming network-centric.

Technology has been one of the central aspects of nuclear material security. To address the growing demand and diverse requirements across India, Kumar said his team strives for standardization and, as much as possible, a standardized process, which is essential for benchmarking and cost-effective systems.

Technologies and Physical Security of Nuclear Materials: A U.S. Perspective

Jordan Parks began by stating that modeling and simulation for physical protection was first done in the late 1980s when the U.S. Air Force began using a tool from Lawrence Livermore National Laboratory called SEES, which simulated force-on-force exercises. The tool evolved into Joint Technical Simulation (JTS) and later into Joint Conflict and Tactical Simulation (JCATS). JCATS was

really the first complete toolkit for modeling and simulation of physical security, and in 1997, it was approved as the official tool for this purpose in the United States. It was used for the Department of Energy, the Department of Defense, the Nuclear Regulatory Commission, the National Security Agency, and the North Atlantic Treaty Organization, as well as some critical infrastructure applications within the Department of State. Most new tools for this purpose today come from commercial industry, but no new tool has replaced JCATS.

In the 1990s, Sandia National Laboratory created a modeling and simulation vulnerability analysis (VA) lab that became the gold standard for VA across the nuclear weapons complex. This lab did both analysis and training. The analyses are based on actual performance determined by testing. Another important aspect of Sandia's approach is the use of subject-matter experts (detection experts, delay experts, etc.) at every level of the simulations to give the highest level of fidelity possible.

Sandia decided to develop modeling and simulation tools for international customers with similar goals, but for different targets, such as critical infrastructure in civilian sites where there were multiple targets versus one highly important target. A lot of the tools in industry do not address issues of multiple targets or multiple paths for attack. When using the same performance-based approach, Sandia had to deal with issues of security classification, but the data for the analysis have to be appropriate to the customer.

Finally, Sandia needed to develop a program that would support its own physical facilities, including one that stored Category I nuclear material. Sandia no longer stores Category I material and that facility is now a kind of museum and training ground to teach physical security.

The VA Process

The VA process can be divided into three broad phases. The first is characterization: Target identifications and whether the target can be stolen or is a sabotage target. What does the threat look like? What are the relevant aspects of the facility (fences, detection systems)? What does the protective force or pro-force look like and how is it trained? What are the tactics? How long does it take the pro-force to get from point A to point B?

Next is the analysis phase. Looking at paths, what is the most vulnerable path from the outside of the facility to the target? What knowledge, resources, or actions might an insider provide that creates vulnerabilities for the facility?

The third phase addresses neutralization and system effectiveness. Using the inputs from the earlier phases, this is where Sandia applies modeling and simulation. Given a detected adversary, given that guards have engaged the fight, what are the chances that the defenders are going to win that fight? That is what the Sandia modeling and simulation tools address, and the results of those simulations help the facility manager or overseer know how effective the system is at countering adversaries.

Moving to evaluation, a facility that achieves acceptable system effectiveness can move into quality assurance and maintenance, making sure to keep a high standard of effectiveness. Those that do not achieve highly enough turn to upgrades to remedy the weaknesses of the system. Then the cycle is repeated to assess and evaluate the upgraded system.

Tools for Analyzing Effectiveness of Protective Systems

There are several ways to conduct combat effectiveness analysis, Parks said. First, there are tabletop or map exercises. These are some of the most common ways of doing analysis, convening subject-matter experts from the site and from the defense forces around a table and war-gaming or working through different scenarios. The strength of this tool is that it gets everyone involved. The rules of engagement can be enforced and the set of scenarios can be limited to those that are plausible.

Limited-scope performance tests, another type of combat effectiveness analysis, test individual pieces of the system—a specific sensor, a specific response time, how long it takes a guard to move from this point to this point—to obtain reliable data for simulation.

Force-on-force may be the highest-fidelity type of exercise, where the security forces war-game through scenarios with Multiple Integrated Laser Engagement System gear, which is essentially elaborate laser tag equipment. Force-on-force is an incredibly expensive and time-consuming type of simulation, Parks said, and the quantity of data are limited. The exercise might be run two or three times. The exercise is an effective training tool for the protective force, but data are too sparse for statistical analysis and system performance assessment.

Constructive simulation utilizes computer models of the facility, the environment, and the protective force and adversaries to evaluate security. The first set of tools is called human-in-the-loop: real people behind computer screens control the behaviors of entities within a simulation; people playing adversaries and people playing defense forces. This is a highly flexible toolkit, much cheaper than force-on-force exercises, and provides more data, but it still requires a week of 15 to 20 analysts' work. Also, as the participants learn from one iteration to the next, they try to game the system, which undermines the independence of the runs: An adversary should not have several attempts.

Finally, there are single-analyst tools that enable one person to build the scenario, build the terrain, build the behavior for the actual entities, press "Play," and allow the computer to run the simulations. These were the focus of the remainder of Parks' talk. Such tools can be more objective in that once the features of the system are set, no humans make decisions, so the results are reproduceable. They can produce large amounts of data. But one is required to have strong artificial intelligence, strong behavioral models, because the aim is to simulate human behavior with no humans involved, which can lead to challenges.

For single-analyst tools to work, the tool needs the ability to build virtual facilities, to build models in three dimensions, utilize artificial intelligence to simulate human behavior, maintain a complex set of behaviors all working collectively, and if possible create visualizations in three dimensions.

Simulation Toolkit and Generation Environment (STAGE)

Parks described a tool called STAGE, which stands for simulation toolkit and generation environment. STAGE is a commercial, off-the-shelf tool from a Canadian company called Presagis. The tool can be purchased in almost every country in the world. It consists of four main tools. STAGE is the simulation tool. Creator Pro is where the user builds buildings and models. AI. implant is a plug-in toolkit that runs artificial intelligence behind the scenes. Terra Vista is the terrain-modeling tool, which can take in high-fidelity geographic information system data and quickly and efficiently build three-dimensional models and terrains for our simulations.

STAGE has a logic-based behavior model consisting of "if/then" statements in a vast library of possible behaviors. Parks said that his team has yet to find a behavior that cannot be simulated in STAGE, and he said that any analyst can learn how to use the tool and build this, without writing code.

AI. implant conducts dynamic path planning, which enables entities in the simulation to navigate between their present positions and their objectives without the user preplanning every action that they can do. The entities navigate around each other and around buildings intelligently. This, coupled with a probability-based combat model and performance-based databases give the user the simulation. Sandia's team has customizable functions that adjust for sensor performance and weapons performance

Because the package runs independently, it can be run in batch mode: 10, 20, 100 runs overnight yielding a large repository of data on the scenarios that played. It can also be run in federation, communicating with other simulations at runtime. For example, STAGE can simulate the adversary force based on artificial intelligence and have actual guards from the facility control protective force in an interactive simulation for training.

With STAGE, a user can simulate each piece of the physical protection system, examining the sensitivity of the system's performance to the performance or that component (a sensor) or subsystem (command and control or situational awareness). The same can be done for the threat. Sandia is beginning to assess insider threats using these models. But it is mostly used in training and in calculating neutralization in overall physical protection analysis and system effectiveness. Sandia has also used STAGE to evaluate the value of potential upgrades.

Parks showed a video clip illustrating the simulations of the Sandia demonstration facility. As the simulation proceeded, viewers saw computer animation of an adversary team breaching barriers at the boundary of a facility and moving to

inner fences, through doors, through the rooms in a building, and then engaging the guard force. Throughout, the tool notes when and where sensors detect the intruders. In the engagements viewers see tracers and in this example the adversary team won the first engagement. At each stage, the simulated adversaries proceed toward their target with realistic time increments for each task, and the simulated guard force responds to signals from sensors and encounters with the adversaries. When there is a failure of the protective system, upgrades to the guard force or the physical systems may be considered and tested cheaply and efficient using this tool.

DISCUSSION

The discussion addressed the flexibility and validation of Parks' model. He noted that he has compared his results for a Sandia facility to some results from JCATS, the standard modeling and simulation tool used in the United States, but he and his team have not compared results to an historical battle. On a related point, **Robert Kuckuck** mentioned in earlier remarks that people who switch from active duty military service with an exciting environment to working as a guard can tend to become bored with guard duty at an installation where attacks seldom happen. **Paul Nelson** asked whether STAGE could account for the effect of such behavior on effectiveness of the guard force. Parks replied that his team generally simulates a fully functional system and not factors like complacency amongst guards, although they can introduce either random or likely delays in response times (e.g., to simulate a guard who was asleep) or reduced performance, but he noted that they generally do not have data to show how frequently that happens. Other participants noted that artificial intelligence has been applied to image analysis or visual analytics, and there are tricks to mitigate complacency, such as having the software intentionally display false alarms, showing an image of a threat object that is not there, as a way of maintaining a certain level of attention.

Participants asked how physical security systems distinguish different kinds of threats and interlocutors. The example of protestors at the Kudankulam Nuclear Power Plant, who have blockaded the gates and at one point approached the plant with a small flotilla of rafts and boats, raised questions about the kinds of threats to these facilities. Are activitists and protestors in the same category of malicious and malevolent actors, like terrorists, seeking to steal nuclear material or sabotage a nuclear facility? The speakers noted that we cannot know what is in the mind of a person approaching a facility. Potential saboteurs can utilize a protest by, for example, mixing with activists and demonstrators to can gain entry. That is why the IAEA and governments see protests as a potential threat.

Participants asked who in the Government of India and in the U.S. Government is responsible for security of these facilities. Kumar replied that the Atomic Energy Regulatory Board (AERB) ensures the design of security aspects

at civilian nuclear facilities. Other nuclear installations, such as BARC, are under the Department of Atomic Energy (DAE), not AERB.

Insider threats were described as perhaps the most critical or the most dangerous threats and a participant noted that most attacks on military facilities in India have been abetted by an insider. With that in mind, what follow-up or on-going verification is conducted on the reliability of an employee after the initial background check? Kumar explained that in India the background verification is a continuous process, with reverification if an official takes up a new assignment or any classified project. Both Indian and American respondents noted that it is the responsibility of managers to continuously observe the behavior of their staff and report if there is a change in the behavior. One participant noted that it is very difficult to affirmatively point out an issue and have agencies look into the matter, and even harder to terminate the employee because concrete evidence is hard to obtain. Typically employees are just moved from a sensitive job to a non-sensitive job.

Another participant asked whether surveillance technologies can help to identify and "get into the mind of" a bad actor. Are there any breakthroughs on how we actually make an assessment when we screen a person and what we do with that screening? Kumar stated that besides the so-called usual measures, there are technical measures—not for monitoring but for neutralizing threats. An Israeli company has developed a questionnaire that it claims can screen for a tendency to deviate from normal behavior. **Philip Gibbs** was not optimistic about the psychological testing because historically it has not always performed well. At a World Institute of Nuclear Security conference, there were lessons shared from the diamond and gold mining industries and applied to the nuclear industry. Among them was the guideline "separate people and gold," which suggests that eliminating the person from the equation entirely at all, where they do not have access to the target or they have access only for a minimal amount of time, may be the most promising strategy.

A participant asked about past U.S.-Indian cooperation on training and other physical security matters. Sandia has conducted international training courses starting back in 1979 or 1980. From that first group onward, DAE has participated, as have some experts from other agencies such as the Ministry of Home Affairs. An Indian delegation visited Sandia's integrated training facility in July 2012.

In a discussion about sensors, such as infrared sensors deployed to detect people approaching a nuclear facility, an Indian participant asked whether India develops its own sensors and whether India has access to foreign suppliers. Kumar answered that in some cases India uses foreign commercial off-the-shelf components and then adapts and integrates those components for India's needs. For thermal cameras, this has been the practice and India is now developing such cameras in Mumbai.

The protective force for civilian nuclear facilities is the CISF, which is a paramilitary force deployed for protection of several kinds of industrial facilities, including airports. In recognition that protecting nuclear facilities is differ-

ent from protecting some other kinds of sites, a set of CISF personnel is rotated among the nuclear installations. They are not kept in one place for more than a certain number of years. **Michael O'Brien** asked then how integrated the facility personnel are with CISF in performing vulnerability analyses. Kumar explained that CISF is part of the response force, so those forces are part of the analysis, and the CISF organization (as distinguished from the guards) is involved in audits and any regulatory review process, including analysis of the DBT.

4

Cybersecurity at Civilian Nuclear Facilities

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- Cybersecurity refers to the prevention, detection, and mitigation of unauthorized attempts to control or disable computers and electronic control systems as well as protections of imformation in compter databases.
- Cybersecurity for a nuclear facility can be divided into two parts: instrument and control security (ICS), and facility network security (FNS). There are several differences between these parts of security, including different methodologies, mechanisms, and the effect of failure in each domain.
- Cybersecurity is commonly understood to have three attributes: confidentiality, availability, and integrity.
- Security risks cannot be reduced to zero. Managing ICS requires a systematic, comprehensive, and dynamic methodology.
- Every day new viruses, new vulnerabilities, and new problems are found with the systems.

Promising Topics for Collaboration Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions are not those representing the consensus of the participants, but are rather a selection of those topics offered by individual participants throughout the presentations and discussions.

- The people involved in the operation of the plant must be sufficiently sensitive to the various aspects of cyber attacks.
- Traditional methods of security for a computer system do not work in environments that have periodic updates and antivirus software; one cannot run intrusion detection programs because of the very limited processing power. One has to build a weatherproof, robust and hardened system. This is difficult to do and is a major area of concern. Solutions exist, but there is a lot that needs to be done in this area in particular.
- The unknown and unused features of commercial off-the-shelf products can lead to significant vulnerabilities. More work should be done on this.

An Indian Perspective on Cybersecurity

R.M. Suresh Babu began by indicating that he would speak about cybersecurity in nuclear facilities in general, which is a broader area, a bigger picture, than speaking specifically about cybersecurity in civilian nuclear facilities. Indian facilities have a large number of computers distributed across the plants, which perform functions from protection of reactor safety to control functions to information collection from displays, and so on. When these computer systems are attacked or hacked by malicious elements, at a minimum certain functionalities of the plant are affected to some extent, and such attacks can lead to serious accident conditions. Cybersecurity refers to how to tackle such problems and how to protect computer bases against malicious attacks by external elements.

Cybersecurity for a nuclear facility can be divided into two parts: instrument and control security (ICS), and facility network security (FNS). There are several differences between these parts of security, including different methodologies, mechanisms, and the effect of failure in each domain. For example, ICS secures safety and control systems such as the reactor protection system, reactor trip system, and power regulation system. While FNS secures the monitoring network, which basically has administrative and managment functions. ICS is applied right from the intial stages of computer-system development and the control-system development. It goes through design development and operation phases, while FNS is most commonly applied during the operation phase of the plant or the facility.

Cybersecurity is commonly understood to have three attributes: confidentiality, availability, and integrity. The impact of a cybersecurity failure or security breach can range from mild to severe to catastrophic if the safety system is affected by a malicious attack. An FNS security failure can lead from mild to severe effects during which data may be lost or transmitted to external persons. With ICS, the most important attribute is integrity. In other words, if the security function is compromised then a serious situation will result. Integrity of the computer system and the software system is the most important aspect of cybersecurity. The availability of safety functions are the next priority.

In the case of FNS, the attributes in priorty order are confidentiality, protection of data, availability of data, and integrity. There is some overlap betwen ICS and FNS. ICS may use some of the functions implemented in FNS to implement certain security controls, but on the whole ICS has to depend on itself and cannot depend on FNS functions or FNS mechanisms.

Following this overview, Babu went into more detail about the ICS. ICS protects the information and communcation systems against unauthorized modification of its resources or disruption of its services. Modification of resources means alteration of software such that safety functions are not allowed to be executed at the required rate or in the required response time. This differs from physical security which deals with the protection of installations, equipment, buildings, and other physical materials.

Security risks cannot be reduced to zero. Managing ICS requres a systematic, comprehensive, and dynamic methodology. Systematic methodologies, Babu said, should build security features into system design and system development processes. He noted that there have been many times when he has detected security-related problems after deploying a system or software, requiring patches. He noted that this is not a good approach because the patches are never a complete solution. There could be a lingering problem with the system. Therefore, when the system is designed, from the very beginning all security features need to be built it in. Also, during the system development process, system verification should address security vulnerabilities, including insider threats such as an attempt to modify software in the development stages. Such scenarios should be considered during the development process.

Second, Babu said that the methodology should be comprehensive, which means it should cover all aspects of the system and its operating environment. For example, a system that is left to operate unattended will require a completely different kind of approach compared to a system that is well protected, and within a restricted area. This should be considered at the time of system design: What devices are used? What is the connectivity with the external world? All of these issues should be considered during the design phase. Failure to do so allows potential attackers to exploit the system.

The third aspect of managing ICS is that it should be dynamic. It goes without saying that the system must be updated as new vulnerabilities appear. The computer operating system, as well as the software and hardware must be made resistant to new vulnerabilities.

There are three components of ICS:

- Security Control: manages the design, development, and operation of the system and consists of a well-laid out security plan as well as policies and procedures.
- Defense In-Depth: so that a single point failure will not lead to a complete compromise of the most critical system, physically security and

cybersecurity must work together to protect the core safety functions against attack.

- Security Lifecycle: similar to System Lifecycle, and consists of several phases of development and verification between those phases; the emphasis is on security and includes configuration management. How are software and hardware being changed during operation and maintenance?

Babu described a recent incident in Mumbai that occurred while a security update was taking place. When the attack was launched, communications with the test server were brought down at the time that the security levels were brought down. It is, therefore, very important that when any changes are made to the system, all consequences of this change are examined along with what precautions should be taken when that system is not available. Update to the control and design should be based on experience; this is another aspect of the security lifecycle.

Security controls should be implemented after having conducted a vulnerability analysis and impact analysis of the system software. Vulnerability analyses help identify other vulnerabilities of the system and the operating environment, and the impact analysis determines what would happen in the event of a security breech in terms of impact on the reactor or the facility or the safety of the plant. Based on the vulnerability analysis, one builds security controls. One also determines what other appropriate controls should be put in place. For example, if the system has a USB or a serial port, then one has to ensure that they cannot be exploited by an outsider. Security controls have to be put in place either to disable them or to make sure that they cannot be used in a compromising manner. Similarly, one must determine the impact to changes in the system that can be made by one person. For example, if the operator can change certain aspects of the system, which will affect only the displaced material, perhaps a one-factor authentication is needed. This is a common issue that does arise and a common means of addressing it in India. However, if an operator is allowed to change a safety set point, then there should probably be two or three factors of indication. Countermeasures, therefore, are selected based on the impact of security failures. These again come under security control of ICS and are fundamentally different from information systems primarily because these systems are deployed in a place where there is no possibility of periodic updates and other functions that are normally done with a computer system.

Finally, the security controls have to be formally defined in a security plan document. This is absolutely necessary, Babu said, because only a plan document, reviewed by all parties involved, can ensure that all appropriate controls are put into place, including the management operational technique of controls (security assessment certification, training, physical protection, access control, audits, authentication, etc.). Babu underscored training because cybersecurity is an area where sensitivity among personnel is not sufficiently developed. “We have to ensure that the people involved in the operation of the plan are sufficiently sensitive

to the aspects of cyber attacks. Unless that is done, it is still possible that someone could create a nuisance."

The second component of cybersecurity is what is called defense-in-depth (see Figure 4-1). In systems that use the defense-in-depth approach, ancillary systems in the plant are divided into various zones. The innermost zone contains very few systems and are those which are most critical to safety and security. The outermost zone contains a large number of systems with a great deal of interconnection between them for systems management and for the collection of information to allow management to understand how the reactor is operating, and other important information.

Between the zones, barriers are created and these barriers become more stringent as one moves from outside to inside zones. The information flow is also controlled more strictly moving from outside to inside. As shown in Figure 4-1, the critical safety system will most likely have very few connections with outside systems, and where there are connections they can only be in one direction. Two-way communications are absolutely removed from this particular interaction through technical means. In effect, demilitarized zones are created where the two systems do not directly interact, rather they interact through an agent, which can prevent attempted intrusions from one zone to the end of the zone. Firewalls are created to prevent certain data from flowing from one zone to another zone. This is a typical example of defense in-depth. The idea is that for a safety function to be compromised, multiple failures in these barriers are required.

The security lifecycle is similar to a system lifecycle (see Figure 4-2). Specified security requirements and controls are developed in conjunction with the verification and validation processes. This is executed rigorously to ensure that all security controls and features are correctly implemented because one has to consider an insider attack.

If certain functions are not implemented correctly, they can become a point from which an attack into the system could be launched, compromising the system. Therefore, there is a phase where verification and validation have to be done rigorously to ensure that the software system that goes into the plant has been verified at the time of deployment when implementing security controls.

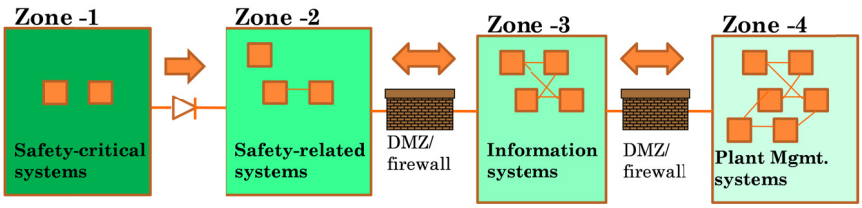

FIGURE 4-1 Defense in Depth for Cybersecurity. SOURCE: Babu, 2012.

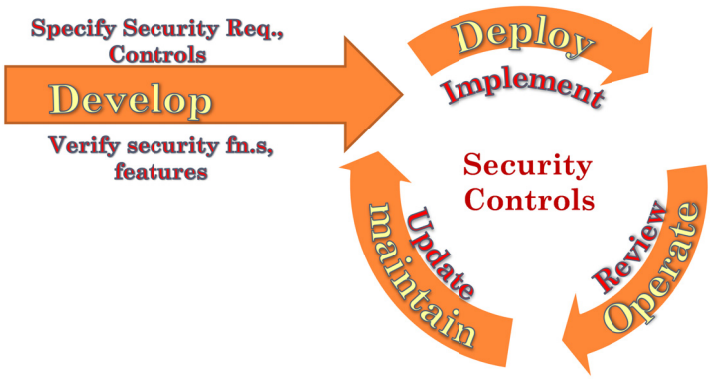

FIGURE 4-2 The Security Lifecycle. SOURCE: Babu, 2012.

The security controls could be different at different points during the development phase and during the operation phase. During the maintenance phase, the system is removed from the specific operating environment. When the security controls are deployed and implemented as well as during operation and maintenance, these controls are reviewed and if necessary updated.

One fundamental difference is that security lifecycles are proactive systems whereas a normal system lifecycle or a software lifecycle is reactive. In this sense, the changes are normally made in the software or the system when certain bugs are detected or when some improvements are required by the user. But with the security lifecycle, periodic reviews are conducted of the entire situation and, if required, designs or controls are changed to address new vulnerabilities. This all happens because the entire scenario is dynamic. Every day, new viruses, new vulnerabilities, and new problems are found with the systems.

One of the main issues of ICS is that they are embedded systems with very limited processor power, limited memory, and have little or no connectivity to the external world. There may be no human admission interface to these systems. As a result, the traditional methods of security for a computer system do not work in these environments that have periodic updates and antivirus software. For example, one cannot run intrusion detection programs because of the very limited processing power. And once deployed, the system is entirely dependent on itself. That is, it has to manage it on its own. Therefore, one has to build a weatherproof, robust and hardened system. This is difficult to do and is a major area of concern. Solutions exist, but there is a lot that needs to be done in this area in particular. Babu noted that the other issue is that about 20 years ago, they deployed custom computer systems that were developed in-house. In the last 10 to 20 years, they have moved toward a more open system and commercial, off-the-shelf components (COT), such as operating systems or hardware available on the market.

The open system concept and COT is a double-edge sword in that it helps to reduce the development time and reduces difficulties of integration with external systems, and there is a large knowledge base and workforce available. But this also can be used by an attacker to cut down or pierce through the system. From a security point of view, there are two problems with the COTS systems. They may have some unknown bugs at the time of system design or deployment. Maybe the attacker already knows a particular bug and can use it to gain entry into the system. There may be certain limitations, which are not known at the time of deployment of the particular COTS hardware or software. It may have hidden functions, which may be deliberate or isolated. This is one area that creates difficulties for the use of COTS in a critical application.

A second problem is that of unused features. If you buy COTS hardware, for example a CPU, it comes with all CDROM drives, USB drives, and a big protocol with an intercommunication software. One may not use all of these features in a particular system, but they are points of vulnerability. They are points through which an attacker can gain entry into this particular system. Therefore, the problem with COTS is unknown features and unused features, and there has to be sufficient protection against these to use the system in a critical application. These are the two important issues on which further work has to be done in the area of ICS.

The second aspect of cyber security is FNS. The main function of FNS is to provide a secure environment for systems to exchange information. There are a large number of monitoring systems: Data from the plant is collected and accumulated for someone to analyze. The FNS must create a secure environment for the systems to interact, which requires continuous monitoring of network activities.

What are the basic requirements for FNS? The FNS must ensure that communication takes place between trusted entities and if anyone tries to connect a new computer to that particular system, the FNS should be able to detect it and disallow the data from going into the connected, internal system. The communication channels should be secured with the use of encryption methods or other methods to make sure that no one spoofs the system and no one attempts to take the data out of this particular network for malicious use. It should enforce established security policies. FNS should be able to detect and isolate malicious programs, devices, and computers on a particular network. These are the basic requirements of FNS.

The Secure Network Access System (SNAS), developed at Bhabha Atomic Research Centre, is shown in Figure 4-3. It has several modules; one of which is the network admission control which detects, identifies, and authenticates the end-system and end-network. Unless the system is supposed to be in the network, it will not allow the system to be integrated into the network.

The SNAS does not allow the system to communicate with other agencies in the network and it forces policy compliance. For example, if some aspect is not compliant with the established policies, then it isolates that particular system. The

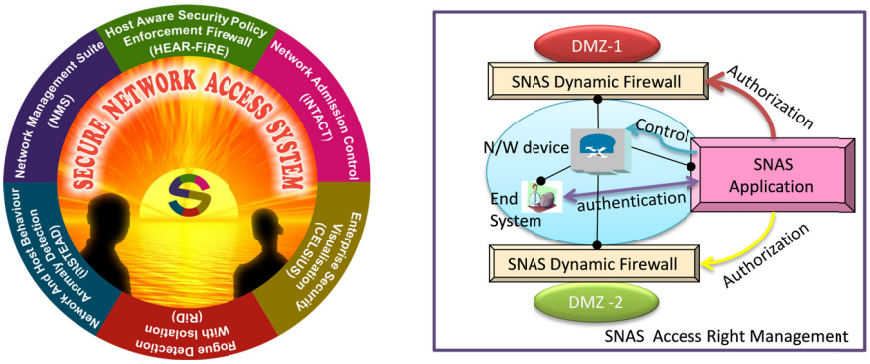

FIGURE 4-3 The Secure Network Access System. SOURCE: Babu, 2012.

other module is network behavior and anomaly detection. It continuously monitors the network and tries to detect whether there is any malicious behavior in terms of network traffic. If there is a certain increase in the network traffic from a particular node or if certain applications are being spawned by this particular system or if there is a denial of service, it tries to look for signatures and behaviors, and tries to isolate those systems.

This is basically for administrators because it allows a network visualization capability whereby one can determine whether or not all systems are connected to the network and what is the state of security is at any given time. The system also allows administrators to know whether the systems are behaving properly or not and if not, they can quickly physically isolate those systems. Visualization is another module that helps implement the FNS requirement.

Finally, another very interesting and important aspect of this system is the firewalls that create barriers between zones. SNAS dynamically changes the rules of the firewalls, depending on the end-system security stage. As long as the system behaves properly, the firewall will allow communication with other systems. The moment that it finds that the security state has changed to an advisable or incorrect state, the SNAS changes the firewall and isolates the system from the particular zone.

On the SNAS console, the intranet is visualized on the screen and one can go into each of the fields, to attempt to determine what other devices are connected to a particular system. It also dynamically displays a particular system if its security status changes through a different icon, allowing the administrator to identify the rogue nodes of this particular system.

Babu concluded by stating that he attempted to demonstrate the important aspects of cybersecurity in a nuclear facility. And also he reiterated the three components of INS and the two main issues on which work is needed going forward in order to tackle and reduce the security risks to nuclear facilities.

A U.S. Perspective on Cybersecurity

Clifford Glantz began his presentation by focusing on the cybersecurity program conducted by the U.S. Nuclear Regulatory Commission (NRC)—responsible for the security of civilian nuclear materials throughout their lifecycle—for all its licensees. Pacific Northwest National Laboratory (PNNL) began aiding the NRC in its cybersecurity work by conducting cybersecurity inspections, visiting four nuclear power plants, and devising preliminary guidance that the nuclear power industry adapted for conducting their own cybersecurity self-assessments and for initiating their own cybersecurity programs. That allowed time for the NRC to go through the long rule-making and regulatory processes. Glantz and his team were involved in providing technical guidance to the NRC for the development of the cybersecurity rule and regulatory guidance. Now the NRC is training its inspectors to start inspecting the plants to ensure that they are in compliance with the appropriate rules and regulations.

The NRC rule is only two pages long and requires the power plants to implement security controls to protect their assets from cyber attacks. In other words, to protect nuclear material and also to protect all the systems responsible for providing safety, security, and emergency preparedness functions at the plants.

The plants are responsible for implementing security and have to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks.

They have to be able to mitigate the adverse effects of cyber attacks and the plants have to ensure that the functions of protected assets or the security of nuclear materials are not adversely affected as a result of a cyber attack.

So the basics of defense and cybersecurity defense are very similar, if not exactly the same as for physical security. One must be able to deter an attack. One wants to keep the bad guys from even thinking about attacking because it would take too much time and too many resoures to achieve their objective. One must be able to detect an attack in progress so that an appropriate respond to the attack can be launched. One needs to be able to delay the attackers from achieving their objectives, and allow time to respond. One needs to deny attackers from eliminating those critical functions that need protection and from obtaining radiological materials. Deter, detect, delay, deny, and respond are key elements of defense both for physical and for cybersecurity.

In the mitigation realm, one wants to be able to resist attacks, to limit the adverse consequences, and to protect confidentiality, and prevent unavailability and loss of integrity of these critical systems. Likewise, one wants to be able to absorb an attack, to take a punch and, if a failure is inevitable, to fail gracefully so that there is time to respond. Also one needs to have the ability to restore functionality in a timely manner. This is very important for a nuclear power plant.

The NRC's regulatory guide 5.7.1 covers cybersecurity. It is about 130 pages long. It provides approximately 140 controls, each with their own set of sub-controls, in 18 different areas. They are divided into three basic families or three

classes; management, operational, and technical. Management involves such things as risk management and system and service acquisition. The operational class covers a whole range of items from developing an effective defensive strategy to defense-in-depth (see Figure 4-4).

Defense-in-depth is multiple layers of defense of a vital area for essential safety and security equipment, a protected area for other systems that are important to operations. There is an outer controlled area, which involves those facilities and assets, which are involved in generating power, for example, when supporting other plant functions. There is a corporate level because most of the plants in the United States are part of corporations that may operate multiple plants so they have several support systems common among their facilities. The publicly accessible area is on the outside. For cybersecurity, this would be the internet, the corporate area would be the intranet, and the company owner controlled area would be a plant network, the protected access area would be critical plant assets, and vital areas—the really essential assets.

Glantz echoed what Babu stated: there are limitations on communication from outside to areas of lower security. From the vital area to the protected area, and from the protected area to the owner controlled area, the NRC requires only one-way communications. Data can only flow outwards. You cannot have information or instructions flowing inward to those particular systems.

It is critical that cyber and physical security zones match up, Glatz said. The NRC is not very clear on this currently, but soon there will be a lot more clarity. One of the concerns is that a facility may have a critical asset with excellent protection, digital protection, but that is located in a place where an unbadged, uncleared staff can get at the digital assets. It makes no sense at all to have A-1 cybersecurity and level C or D physical security for that particular asset.

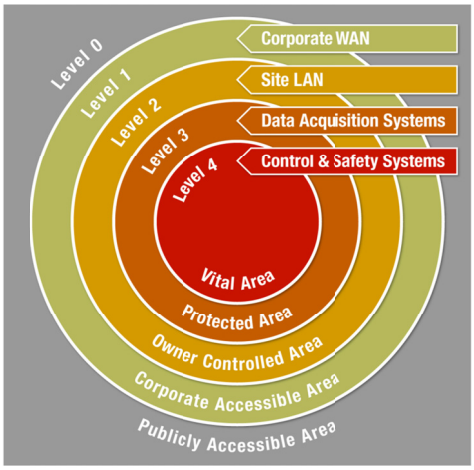

FIGURE 4-4 Full Range of Cybersecurity Measures. SOURCE: Glantz, 2012.

The other areas of operational control include awareness and training, configuration management, maintenance, and, very importantly, media protection. Also important are contingency planning, incident response, personnel security, and physical and environmental protection, which involves maintaining the critical infrastructure that the digital devices need to survive. Electricity, heating and cooling, appropriate fire protection and other support systems cannot be overlooked.

Appropriate security awareness and training is essential, as illustrated by what appears to have occured at the Iranian nuclear facility. Appropriate media protection is also necessary. Media from one level should not be moved into another, higher level of security. Personnel security is another issue. When one hears about the insider threat, one often thinks about malicious threats. What is the insider doing with the intention of causing harm? That is very important, but there is also the non-malicious threat posed by insiders. Effective cybersecurity programs must protect from both malicious and non-malicious insiders that can result in adverse consequences.

Finally, the third class of controls is the technical class, including access control, audit and accountability, identification and authentication of users, communication protection, and system hardening.

Glantz also discussed the importance of integrating physical security and cybersecurity. Before someone breaks into a facility, they will most likely conduct something along the lines of a cyber attack to disable the physical security system. If one is planning an attack against a fortified facility, what better way to defeat the digital physical security controls than through a cyber attack, rather than just a purely physical attack?

This just illustrates that there are many attack vectors to get to assets that an attacker might want to reach. The attacker wants to maximize the probability of success while minimizing the possibility of getting caught. So they are going to take the path of least resistance that achieves their objectives and it doesn't matter whether that involves a physical attack, a cyber attack, or a combination of both.

The basic concepts of physical security and cybersecurity are essentially the same. For example, with physical security there are fences, for cybersecurity there are firewalls. Basically, they fulfill the same function. For physical security, there are perimeter patrols to ensure that the fences are doing their job in keeping adversaries out. For cybersecurity, monitoring of firewall logs is needed to ensure that attemped break-ins are detected, and that they are not given unlimited time to defeat the defenses. Keys and passwords are analogous, both use intrusion detection methods, both physical and cyber, and both have incident response teams.

The protection systems around nuclear facilities, be they power plants or any facility involved in the fuel lifecycle, have on array of digital controls that are part of this system. In the United States, facilities have various alarms and detection operating between fences. There are admission stations into the facility where access is computer controlled. There is a database that is accessed to

ensure that each person entering has appropriate credentials to enter the facility or the particular security zone.

Physical security programs are increasingly using more digital devices to improve their productivity and efficiency, but one must be aware that this introduces new vulnerabilities into the system. Physical security systems require cyber security to ensure the availability and integrity of their functions. They need to avoid the spoofing of surveillance cameras and other monitoring equipment. Those cameras should show what is actually going on and not what was going on 30 minutes ago or the previous day. One must also avoid alarms being digitally silenced, and alterations to access control data bases and interference with security communications. Physical security systems need to be protected from both physical and cyber attack. Digital systems require physical protection. Again, they need to be held to the appropriate security level to avoid theft or physical damage of critical digital systems, or unauthorized access to those devices or the disruption of their critical infrastructure.

Many vulnerability assessments involve exclusively physical examinations of the physical domain. They are often done by physical security experts. In the cyber domain, cybersecurity experts will examine what is going on to assess vulnerability, but very seldom are total security assessements conducted, during which both the physical security and cybersecurity are examined in the areas where they overlap. There is an important need to integrate these physical and cyber vulnerability assessments and to have the physical security experts and cybersecurity experts working together to develop an effective security system. We need to defend against physical attacks, cyber attacks, cyber-enabled physical attacks, and physical-enabled cyber attacks.

PNNL is developing a tool called Pack Rat. Pack Rat stands for "physical and cyber risk assessment tool." It uses some of the quantative tools widely used for physical security risk assessments and adds a cyber component. Instead of just looking at the physical security pathways and the time delay provided to the defense force to counteract a physical attack, it also looks at the cyber pathway as well, of entering and attacking physical security systems, the time delay that those cybersecurity measures provide and integrates that with the physical security for a more coherent picture. This is a very interesting tool that is in the final testing phases and will soon be a candidate for commercialization. This is an example of the tools that are needed to integrate physical security and cybersecurity.

DISCUSSION

During the discussion period, a participant noted that one of the statements that U.S. President Barack Obama made in Prague was that the clear and present danger today is nuclear weapons falling into the hands of terrorists. That was his nightmare and as it turns out, it has been a nightmare for India planners for some years now as well. Forensics and cyber/physical security are areas of cooperation

where those at the workshop would do well to note and perhaps put down as a suggestion for future engagement. There have been reports that the security systems of India's neighbor, Pakistan, are top-notch. But that is not the problem in Pakistan. Who are the people in control? What is their loyalty? Did they not indulge in one of the largest nuclear black markets in the world that anyone has ever seen? Those traces of highly enriched uranimum found in the centrifuges in Natanz are indicative of the problem. If the United States and India could have solid data sharing on this issue, it would be a great step to bring about an end to Obama's nightmare the participant said.

Glantz noted that there is a dramatic change in threat vectors. The capabilities of potential adversaries are advancing at a faster rate than our ability to defend our systems. This emphasizes the need to have defense-in-depth with multiple layers of defense available to protect the systems. Hopefully the vendor communities are starting to slowly make security an important element in their control systems. But the digital control systems live for a long time in facilities. They are very expensive to replace and so the critical infrastructure has to live with these vulnerabilities for the foreseeable future and we have to take those defense-in-depth steps necessary to deny attacks from actually reaching these vulnerabilities.

Babu added a few points. There was a time when safety systems were all hardware. Then, people began introducing digital computers into safety systems. Now there is an Indian regulatory requirement that critical safety systems completely run on a computer, one must have a parallel system, which would be completely different. Would it not be subject to the same common requirement as a digital system for the most critical safety functions? In one sense, Indian regulatory guidelines and designs ensure that nothing catastrophic will happen in case of a cyber attack.

Further, as people become more and more aware of cyber attacks, controls are being built into digital systems. For example, the systems that are made in India, even though they may be customized systems, may have unnecessary features, functions, and devices, are now becoming more and more resistant to attacks.

A workshop participant asked about cyber offense as a weapon. Should we not also take measures to protect ourselves? Shouldn't we look at cyber offenses as well?

In response, another participant said that if one is threatened by nuclear weapons, surely one of the weapons in a country's armory should be cyber weapons. Law is not a problem because if a country is attacked it has the right to self-defense.

Glantz noted that attribution of a cyber attack is difficult. One can suspect where the attack comes from, but it takes a lot of time for digital forensics to determine with close to absolute certainty, where it came from, if it is possible at all to know. There are instances where someone mounted a cyber attack against a country and disguised it so that it looked like it was from their adversaries, and therefore used it to provoke escalation of a conflict between the two adversaries.

Therefore, like any offensive weapon, one has to be very careful about how it is used. There is the temptation for political leaders to respond to a severe cyber attack in kind, and do it before they have full information as to where that attack may have come from.

A workshop participant asked whether or not a cyber attack like the kind that happened with the Stuxnet it is an act of war? Does international law recognize this as an act of war? Right now it does not, although it should, the participant said, because attacking an oil installation with bombers is an act of war. It is time to modify international law such that these acts are considered an act of war. There is the problem of forensics, but in the case of Stuxnet, everybody agrees on the origin. It is a straight act of war. Why isn't the international community able to do something about setting up a framework to make these acts of war such that retaliation is allowed by international law? Another participant added that it was declared an act of war in June 2010 by the United States—not Stuxnet but cyber attacks. Glantz noted that he does not think there is a limitation on nations working together to develop appropriate responses for cyber attacks or to work on defense. His only caution is that unlike an attack from a marked aircraft, where you know right away who is attacking you or whose missles are incoming, where you can track on radar where they are coming from, a cyber attack comes and it is written in computer language and it spreads around the world even though it is targeted against one particular system or one particular country. Stuxnet was found in computers all over the world, including in India and in the United States. Stuxnet would wake up and look around and say, where am I? If the local language wasn't Farsi it shut itself off. Then it would wake up and say, well it is Farsi, but it looks like I am in a water plant and it would shut itself off. It was only looking for one location and one type of digital controller and then it did its work. It is very important to have the correct attribution, which is extremely difficult. We could have escalating conflicts all over the world that are starting up not because some country actually attacked another, but because some other country disguised it to take advantage of a situation, that conflict between other countries.

A workshop participant stated that the topics of cyber warfare and cyber defense are very modern topics. It is indeed an area in which individual nations, let alone the community of nations, have yet to really formulate the rules of the road, the rules of engagement, and so on. But clearly, basically all nations recognize that there is a need to do so first internally and then internationally. So it is just the beginning of an effort that is necessary and that necessarily takes time. People in the United States are trying to consider these issues at the government and business levels. The U.S. National Academy of Sciences has conducted a few studies in this area, one which was published three years ago. We are really just beginning to formulate some of the questions having to do with cyber attacks.

The point about attribution cannot be overemphasized, and quite frankly, a standard mode of operation is for an attack to be perpetrated through another computer system, stated a workshop participant. Speaking completely hypo-

thetically, even if a computer system under attack can recognize where the attack is coming from and go after the attacking computer, the owner of that attacking computer may have no idea that their computer is doing the attacking. So to the degree that one could isolate or quarantine that computer system, that in fact is an attack on it. From the owner's point of view, the participant noted, that is an attack. There are some subtleties here that really have to be thought through as to what is considered legitimate defense and how to deal with this internationally, and what kind of agreements we have. This is urgent, everyone realizes this, but it is really not simple. It is a very subtle and complicated issue. In the United States, there is quite a national tension between the government views of what needs to be done for protection, which may include what is viewed as an attack, versus for example, the business community's views of their needs for structure, let alone what the public at large feels are our collective needs. This is an area where we could have very productive, intense discussions between the United States and India.

A participant asked whether, as part of defense, it is possible to develop any special computer languages that are more resistant to such attacks? Is it part of the program by any chance?

Babu noted that actually it doesn't depend on the language. It depends on the programability of the computer itself. That is where the hole is, so, yes, by using a special language, maybe one can build that security hole in the software itself. Maybe you can design a language. But there are still hardware issues, such as a USB drive in the system. One has to take care of the operating system, to harden it so that vulnerability points cannot be misused by anyone. There is a combination of internet software, which runs in a computer including the operating system, the drivers, and the appliction software based on a language. It is very complex.

A participant asked Glantz to clarify the implementation of the NRC cybersecurity rule at U.S. power plants. Glantz explained that the implementation of the NRC cybersecurity rule and regulation is for all 100 plus reactors in the country. Inspections will begin in January 2013 as the initial implementation of the program. By 2016, it is to be fully implemented and the inspections that are conducted at that point will have full regulatory authority, including the ability to levy fines and shut down plants if they don't fully comply with their cybersecurity requirements.

He also agreed with other workshop participants about the urgency of the issue, but noted that operating systems in the United States are improving and becoming more secure. There is also the issue of flaws in the actual software that is used on U.S. systems, both digital control systems and other enterprise network systems. If one thinks about some of the large codes used in software packages, they are thousands, hundreds of thousands, million of lines long. Because they are developed by human beings, they have design flaws and coding bugs in them as well. That means that no matter how much we have security in mind when that software is written, we can never be 100 percent sure

that there is not a vulnerability and that a skilled hacker, a skilled attacker, can not take advantage of a vulnerability. There is always that possiblity.

A workshop participant asked Babu about a system as it is being developed. He replied that, yes, when security is built in up front, one sees many malfunctions, and there are advantages of not using such systems. When one considers where the attack vectors are for example, an attacker wants to exploit whatever is possible. The attacker is looking forward, for openings. A defender is looking at the past, where an attacker has gone, where the attacker has exploited.

Generally, security and cybersecurity are not thought to be tenable. It is not something you can take for granted. We can say we have closed all attack vectors, but what about the people who are involved in the development? When they go, where do they go? What happens to them? Their knowledge goes with them. Is it possible that someone could have no product with him but has knowledge that can be exploited?

Babu replied that, yes, this is a hot topic, involving insider attacks and outsider attacks, and the most fatal one is the combination of insider and outsider attacks. They are aware of this kind of threat. All software is reviewed by a third party. They have teams who double up intrusion-attack test cases where they try to inject malicious software into the operating systems. Third party verification is a very important part of the qualification process. When a third party looks at it, they may have a completely different perspective on how the system can be exploited.

As far as an insider attack or the knowledge base that leaves is concerned, it does not create much of a problem as long as one ensures that the systems are untamperable. For example, the first software base was from India, and the system cannot be tampered. The software cannot be changed. Even if I want to change it, it is not possible. So as long as one takes care of the security controls and puts in countermeasures, considering the possibilities of attacks and other possibilities in the future (how the system will be used), and as long as they are reviewed by third parties, one can be quite sure that the risk involved will be reduced.

It is an evolving technology, and an evolving methodology. There is no final answer. There is no full-stop in cybersecurity. One must now think about how people have developed the technology and are going to exploit it in the future. The lifecycle must be continuously reviewed and countermeasures put in place at appropriate times.

Paul Nelson asked if there is some limit to the solution by means of adding more layers? For example, as one adds more layers, the number of pathways through the system tends to increase exponentially with the number of layers and that would make verification validation studies more difficult. Is that an issue? Is this a realistic issue in current practical systems?

Glantz replied that the five-layer system developed with the NRC seems to make sense from an industry or plant-operation standpoint, based on the communications that they have to have and the different levels of trust between

those various types of communication. Clearly if one has more layers than one needs, this is economically inefficient. All of the cybersecurity controls tend to have their draw backs. One of the controls is conducting intrusion detection, which is valuable, but then one has to think about communicating that intrustion detection information back to security specialists, which opens up potential new lines for security.

Some corporations that opeate nuclear power plants have decided that the matter is most efficiently handled by people at the corporate office. So now these people at the corporate office have access to firewalls and intrusion detection systems that are in the inner layers. There are active discussions going on about that right now: what is acceptable and what is not acceptable. As security is added, be it layers or something else, one has to be very mindful of the vulnerabilities that such security control may introduce into the system.

A workshop participant asked to clarify whether or not an attack can happen during the time the security update is occuring. Is the attacker conscious of when the security update is being done or does it mean that the attacker is looking to attack all the time? Babu replied that this happened in Mumbai when they were trying to update their software to introduce more antivirus capability. While updating, what happened is the security level was brought down and an insider logged on at that particular time between 11:00 and 11:30 pm. With this information an external attack took place. The most fatal one is where an insider collaborated with an external attacker and logged on and then launched the attack. It becomes extremely difficult to track in this case.

Glantz replied that one of the major issues is where a good system is built with firewalls in the right place and an appropriate rule set, but they do not invest in actually looking at their firewall logs on a regular basis. Maybe they will do it every 30 days or 60 days or maybe they will give it a superficial look. A cyber attack could be an ongoing, non-stop, 24/7, automated attack, just waiting for that security level to drop or a vulnerability to show up that it can take advantage of. Those attacks are ongoing all the time. If attackers suspect that there is a vulnerability, they will keep pinging at it until defenders detect it and do something to stop that threat vector from going forward.

A participant picked up on the other aspect of that question: How well or poorly can one authenticate the updates themselves? It seems that the updates could be a pathway into the system that might not be checked. Babu replied that normally updates come with digital signatures. There are ways to authenticate that it is coming from the right source. That could be a vulnerability point, but there are methods to take care of that.

5

The Importance of People in Securing Civilian Nuclear Facilities

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- Every person, from a custodian to a technician to a scientist to a guard in the protection forces, needs to believe in and support the nuclear security program for it to succeed. This is nuclear security culture.
- The driving motivations for the Indian Global Centre for Nuclear Energy Partnership (GCNEP) are first global cooperation and second the technical issues of safety, security, and proliferation resistant design as the three pillars on which the Centre will stand.
- Specifically, the GCNEP School for Radiological Safety Studies is designed to contribute significantly to nuclear security, particularly in the area of radiation sources.
- Unless we update ourselves, unless the security forces, the response forces, the guard forces, and the security operators update themselves with the current threat scenarios, with current practices, with current systems, and techniques used, and also with required regulatory procedures or other requirements, it will not be possible to maintain proper and effective nuclear security.

Promising Topics for Collaboration Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions are not those representing the consensus of the participants, but are rather a selection of those topics offered by individual participants throughout the presentations and discussions.

- There are several training and licensing issues, particularly for the protective forces, still to be addressed or improved.
- A pathway to success in cooperation is training, and there are many opportunities for cooperation between India and the United States on multiple issues associated with the human aspects of nuclear security.

The Important People: An Indian Perspective

Ranajit Kumar began his remarks by stating that it is important to train personnel on security procedures. Physical protection security (PPS) technologies—hardware, detection, access control, assessment, surveillance and other technologies—must be backed by appropriate security policies and procedures (see Figure 5-1). Training is vital for effective implementation of nuclear security. In most cases, training is neglected. In fact, the time has come to be very stringent on the aspect of training qualification and licensing issues, he said.

There are certain guidelines and there are many efforts by the International Atomic Energy Agency (IAEA) to take this training aspect of nuclear security to all member states, but the member states also have a significant role to play. During the course of the presentation, Kumar highlighted some of the activities that have been carried out in India and to which India is committed, including participation in the IAEA effort to take nuclear security training to different member states and to make it really global. It is important that nuclear security concerns are addressed globally. One state cannot address this problem and consider itself out of danger from nuclear terrorism or other nuclear security concerns. Kumar reiterated that nuclear security issues have the potential to have effects beyond the border of the originating state. Nuclear security concerns are not limited by any geographical or political borders, therefore, they should be taken seriously and much more effort needs to be taken globally to ensure effective nuclear security.

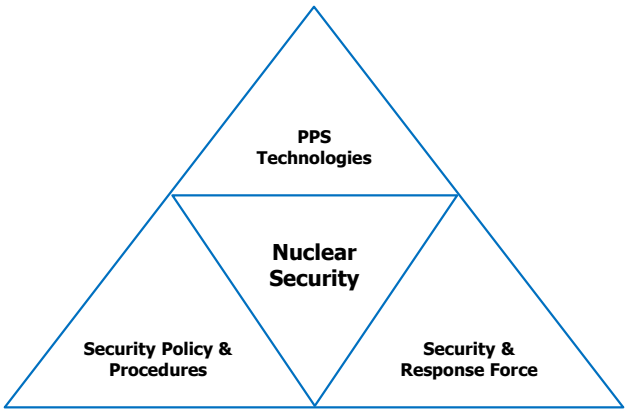

FIGURE 5-1 Integrated Security Approach. SOURCE: Kumar, 2012.

Nuclear security is very multidisciplinary. There are science and technology components, which are always a part of nuclear security issues, for example in the usual nuclear material accounting procedures and processes, and instruments and systems. In addition, there are various social science elements which need to be understood, analyzed, and applied. This pertains, for example, to human or personnel reliability programs. A personnel reliability program is a program in which one looks at the social background or the societal aspects of a person; how he is living, how his behaviors are changing. Several studies address these issues that go beyond science and technology issues. These are societal issues that are under active research. There is a broad range of social science aspects, including public policy and political science issues, international relations, and international law. There are also obligations as well, such as United Nations Security Council Resolutions. A state analyst for international transport should also come into the picture in such instances. There are questions about what to do if there is no budget for these studies. The essential point is that nuclear security is a multidisciplinary subject and it requires the right mix and the right attention to differences among the social science and physical science issues.

Why do we need training? Training is required to increase awareness. Based on his experience, Kumar observed that perhaps 10 to 15 years ago, if one would have asked most of the people present here whether they would be sharing advice about nuclear security, they would have said that it is the guard forces' responsibility. "Let them bother about it." But mostly the response would have been something like this: "Security incidents will take place in some other place. There is no belief that a threat really exists." This is something that people needed to be made aware of.

With respect to specific training, one has to address the requisite skills. For example, when one is doing a search, what is the search, what are you looking for, how is the search to be carried out without becoming too much intrusive? Similarly, when one is talking about an operator who is in the central alarm station, what are the requisite skills needed that can be developed specifically by providing training? Skill sets also need to be upgraded when required - training just once does not help. One must train and retrain, qualify and requalify; that is what is required.

For safety issues, training is also a regular process. Operators are trained and then they are retrained, reexamined, and revalidated for licenses. This is also the requirement for nuclear security operators and for the response forces. There are several training and licensing issues.

One needs to assist in capacity building, training, and finally in human resource development. Continuous training and improvement is key to effective nuclear security. Nuclear security is a very dynamic issue. Threats are also dynamic.

In order to make the training more fruitful and to incorporate global participation in training, Prime Minister Manmohan Singh, stated during the 2010 Nuclear Security Summit, "I am happy to announce on this occasion that we have

decided to set up a Global Centre for Nuclear Energy Partnership (GCNEP) in India. We visualize this to be a state of the art facility based on international participation from the IAEA and other interested foreign partners."[1] His remarks go on to state, "The Centre will conduct research and development and design of systems that are intrinsically safe, secure, proliferation resistant and sustainable. We welcome participation in this venture by your countries, the IAEA and the world to make this Centre's work a success."

The main driving forces for the Centre are: 1) it is for global cooperation and, 2) the technical issues of safety, security, and proliferation resistant design are the three pillars on which GCNEP will stand (see Figure 5-2).

Five schools have been established in GCNEP, around which these activities will occur:

1. School of Advanced Nuclear Energy System Studies
   a. Objective: to pursue design studies and analysis of advanced nuclear energy systems with intrinsically-enhanced safety and security for proliferation resistance and sustainability.
   b. Training Focus: Risk assessment studies, emergency planning and management, sustainability parameter assessment, different aspects of safety, security, and proliferation resistance, evaluation of performance indicators and safety, security and proliferation resistance, regulatory process, safety culture, radiation protection, and nuclear law.

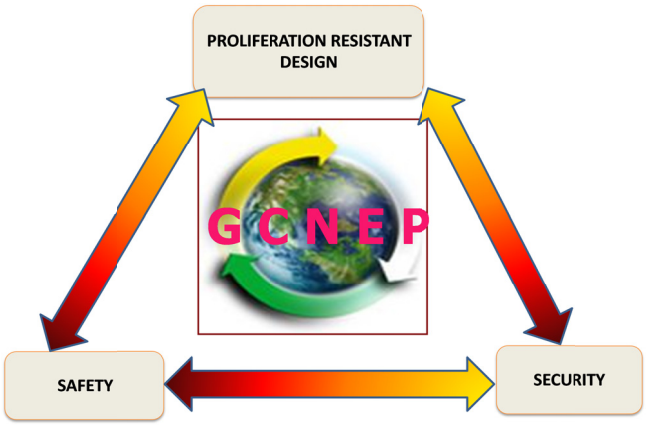

FIGURE 5-2 The Three Pillars of the Global Centre for Nuclear Energy Partnership. SOURCE: Kumar, 2012.

[1]Statement by Prime Minister Manmohan Singh at Nuclear Security Summit, Washington D.C. 13 April 2010. The Hindu. Available at: http://www.thehindu.com/news/resources/statement-by-prime-minister-manmohan-singh-at-nuclear-security-summit-washington-dc/article396372.ece. Accessed on September 21, 2013.

   c. Program Modules: reactor systems and applications, fuel cycle studies, accelerator driven systems, risk assessment studies, emergency planning and management, and sustainability parameters assessments.
2. School of Radiological Safety Studies
   a. Objective: to carry out research and development in radiation monitoring including development of detectors and systems; to develop the system to support nuclear emergency management; to contact radiation transport, selling, dispersion modeling and impact assessment studies, and to impart training and certification of personnel in radiation protection principles and safety practices. To maintain and update radiation protection standards.
   b. Program Modules: formal education, training, and public awareness, response to a radiological dispersion device, a radiation exposure device and other radiological emergencies, radiation mapping by mobile monitoring systems, source search, detection, identification, assessment and recovery, lessons learned from nuclear and radiologic al accidents, studies on dispersion of atmospheric and aquatic releases.
3. School for Studies on the Application of Radioisotopes and Radiation Technologies
   a. Objective: to provide state of the art research and development and demonstration and training facilities in the application of radioisotope and radiation technologies.
   b. Program Modules: formal education and training, radiation processing of food commodities, value addition to healthcare, medical and herbal products, radiation induced enhancement in properties for creating advanced materials, industrial radiography and tomography using gamma and x-rays, radiotracer and isotope use for high technology systems and managing water resources, waste water treatment.
   c. Training Focus: food irradiation, material processing, waste-water treatment, x-ray, gamma radiography, tomography, radiotracer and isotope instruments, nuclear forensics.
4. School of Nuclear Material Characterization Studies
   a. Objective: to promote research and development (R&D) activities for evolving new methodologies to detect and ascertain the causes for unaccounted losses of nuclear materials on a timely basis; to establish a teaching and training facility for the effective implementation of safeguards including nuclear material accounting and control (MC&A) and its practices at national as well as international levels; to establish an advanced infrastructure and demonstration facility for human resource development in the practices of nuclear material accounting and control; to create a versatile secured data management system for MC&A.
   b. Program Modules: methodology for destructive and nondestructive analysis of nuclear material; formal education and training on MC&A; development and validation of trace elemental analysis techniques;

and development of methodologies for low level detection of radionuclides.

5. School of Nuclear Security Studies
   a. Objective: to impart training on application of physical protection system and response procedure, enhanced physical security of nuclear facilities by developing and deploying most modern technological tools including information security and to provide facilities for test and evaluation of sensors and systems used for physical security.
   b. Program Modules: formal education and training; technological tools for physical security; personnel reliability studies; vulnerability studies; seismic monitoring; and test and evaluation of sensors and systems.

Kumar expanded in more detail about the School of Radiological Safety Studies (SRSS), which is designed to contribute significantly to nuclear security, particularly in the area of radiation source security. The mission is to carry out R&D on radiation detection systems and dosimetry. A great deal of work is being carried out at Bhabha Atomic Research Centre (BARC), in Kalpakkam, and in several other institutes across the country. GCNEP is an effort to consolidate some of these activities and to encourage global participation.

The goals of the school are to: affect the assessment of radioactivity releases integrated with geographical information systems with nationwide radius and background mapping; ensure the safety of radioactive nuclear material; address emergency preparedness and response, medical management of radiation emergencies, and conduct fixed field exercises on radiological safety, and emergency response. Specifically, different program modules (formal education) are envisioned. Studies on radiological dispersion in the atmosphere are also planned, as are studies on indigenous systems already developed, such as in searching for orphan sources. Similarly, the SRSS will work on the indigenization of systems for assessment of large area contamination, detection of smuggling or inadvertent movement of radioactive sources or nuclear materials in scrap, cargo, or vehicles. Most of these systems have been developed and deployed on a pilot scale at some of Indian ports, which are the systems for entry and exit control. Not all areas are currently covered.

The SRSS will also house an emergency response center. There are currently 12 emergency response centers across India, and they are monitored by the emergency response monitoring network, and have all the modules for mobile and aerial searches, monitoring at ports, and a facility for air monitoring of stand-alone detectors, which communicate using the Global System for Mobile Communications (GSM) or Code Division Multiple Access (CDMA) networks. There are more than a few hundred: Kumar estimated that around 500 such detectors have been deployed all across the country. There are plans to expand this significantly. They will report to the regional centers, and then they will report to the Emergency Response Center in Mumbai.

Kumar reported on the radiation safety training courses currently provided by BARC (see Table 5-1).

Kumar provided more description of these courses. For example, a course for first responders to nuclear and radiological emergencies would include training of trainers, and management of crime scenes involving radioactive material. Similarly, on the order of 45 training courses are conducted for radiation therapy technologists. Some of them go for a one-year radiation therapy degree leading to a diploma. Some of the training courses conducted in radiological safety are for the National Disaster Response Force, state police, firefighters, civil defense, Department of Atomic Energy (DAE) Emergency Response Team, and medical professionals. In the middle of October 2012, there was a training course on medical emergencies in Mumbai. Similarly, import and export agencies, front-line officers such as customs officers, and radiation safety officers of nuclear facilities, medical institutes, industry, and researchers. Kumar noted that they are trying to extend these courses as far as possible, including to the universities under the Homi Bhabha National Institute (HBN1).

In cases where conventional explosives were used, there is an India National Disaster Response Force (NDRF) that could be called at the request of the state authorities or of the Indian national government. The NDRF conducts analysis to determine whether a radiological dispersal device (RDD) element was present. In many cases, other teams would also help in carrying out analysis. There are many developments, particularly in the area of radiation emergencies, specifically on how to handle radiological materials, how to do first response, and how to conduct medical responses.

The School for Studies on the Application of Radioisotopes and Radiation Technologies is included because of the desire to make GCNEP a complete Centre also addressing other activities apart from nuclear security or safety. In order to be viable, the GCNEP has to take the technology, and in particular the application of nuclear technology, to the public and to the regional level. Established near New Delhi in Haryana, the Centre envisions being an applied center so that the people in nearby communities can benefit from the application of such techniques.

In particular, Kumar said that there are many applications of radiation in sterilization of medical products and in processing food, such as spices. Therefore, they wanted to include those issues in the particular training courses and train local people as well as address global health should it be required. Many of the courses offered are organized in association with the IAEA, particularly nuclear medicine and food and agricultural processing.

The School of Nuclear Material Characterization Studies aims to promote R&D activities, to establish a teaching and training facility and to establish an advanced infrastructure and demonstration facility for nuclear MC&A and to create a versatile, secure data management system for MC&A.

The School of Nuclear Security Studies plans to provide formal education

TABLE 5-1 Radiation safety training courses currently provided by BARC.

Serial No.	Name of the Course	Duration	Eligibility (Science Graduates)
Emergency Preparedness and Response for Nuclear and Radiological Emergencies			
1.	Response to Nuclear Disaster/Radiological Emergencies	4 days	Defense Officers
2.	First Responders training workshop on response to nuclear/radiological emergencies	One week	Paramilitary Forces
3.	Training of Trainers course for Paramilitary Officers	3 weeks	Paramilitary Forces
4.	Prevention and response to radiological emergencies and Standard Operating Procedures	One week	Police Officials
5.	Prevention of malicious acts using nuclear/radioactive materials	Ten days	Forensic officers, Police, NSG, Defense officers
6.	Aerial survey and field exercises	4 days	Defense Forces
7.	Nuclear and radiological emergency management	3 days	NSG and other security agencies
8.	Training workshop for Emergency Response Teams of DAE	3 days	DAE officers
	Industrial		
9.	Radiation Safety Aspects for RSO in Nucleonic Gauges	7 days	Degree in Science or Degree/Diploma in Engineering
10.	Industrial Radiography Testing Level-I	15 days	High school diploma with two years of prerequisite education, science/diploma in engineering, and 6 months of work experience
11.	Industrial Radiography Testing Level-II	15 days	RT-I and 36 months of work experience
12.	Radiation Safety Aspects for RSO in Radiation Processing Facilities	3 months	Degree in Science
13.	Radiation Safety Aspects for Operators in Radiation Processing Facilities	3 months	Degree in Science

SOURCE: Kumar, 2012.
DAE: Department of Atomic Energy
RSO: Radiation Safety Officer

and training programs in this area. Kumar noted that a graduate level program would be started in the future, but a beginning will be made with formal education in this field. Use will be made of the technological tools for the study of physical security, as well as personnel reliability studies, vulnerability analyses, seismic monitoring, and the test and evaluation of sensors and systems. The R&D focus will be on research in the frontier areas of security equipment, systems, and sensors. The proposal is to address performance testing and evaluation of systems and sensors, particularly the applicability of these technologies in India and countries of the region. Training and exercises will also be undertaken for security and guard forces, training of plant personnel on security issues, and the development of table-top and near-real-time simulations and field exercises. The plan is to set up computer and information security training as well.

The R&D activities of the school will emphasize cybersecurity, particularly applicability for secured information exchange and to PPS. Kumar noted that they have already conducted several departmental training courses in system design, and training for plant maintenance personnel and operational training to security personnel. A great deal of experience has been accumulated in conducting international training courses. Over approximately the last 10 years, eight to 10 training courses have been held in association with the IAEA primarily on the aspects of design of physical protection systems and vital-area identification and the like.

In conclusion, Kumar stated that nuclear security is a national function, however, its implications extend beyond the states' borders. Effective nuclear security requires continuous training, and improvement is a must. Nuclear security and safety measures lead to a strong culture where improvements are an ongoing, regular process. India contributes significantly to the IAEA on issues related to nuclear materials security, and the new Global Centre for Nuclear Energy Partnership will take this farther by providing training to people in India and around the world.

Training on Nuclear Materials Security: A U.S. Perspective

Michael O'Brien began by reiterating that training is an extremely important subject. It is essential in all aspects of security. Through the years, its importance has grown throughout the U.S. Department of Energy (DOE) and the National Nuclear Security Administration (NNSA), and therefore O'Brien presented the U.S. domestic program for security training within the DOE complex and how that has brought forth international cooperation and related training.

The National Training Center (NTC), located in Albuquerque, New Mexico, provides security and technical training. It does not provide a formal education, but serves the purpose of keeping all personnel within the DOE complex up to date on modern technologies and techniques. The NTC has classroom facilities and they also conduct remote learning via the web. They will also do mobile training, so if a facility has a training need and sufficient numbers of students, an

instructor will actually come to one of the laboratories and teach a class. They also offer correspondence courses for those people who may want to migrate into a different field of security.

In addition to the NTC, all DOE sites have their own training programs. They are all fairly uniform. The primary focus of security training is on the protective force. There are many requirements for the protective force. Employees themselves are also trained. There are security awareness programs for people who work within the DOE complex, which are required annually as refresher courses on security awareness. O'Brien commented that as he listened to Kumar's presentation, he began to consider whether computer-based courses are the best way to take annual refresher courses given the importance of security awareness training and security culture. In years past, guest speakers came to the labs and provided real-world experiences and maybe that has a greater impact. The U.S. national labs also have on-the-job training that is very consistent with the tasks performed by people who service U.S. systems. These employees are usually mentored in their jobs, which is referred to as training. There is also commercial vendor training, if there are new tools involved. Recently, a vendor came to Lawrence Livermore National Laboratory to look at a vulnerability assessment tool that could be exported internationally.

The NTC focuses on the management of security, so there are some courses that supervisory personnel can attend and learn about managing security at U.S. sites. But they also train the instructors themselves. Therefore, these are good courses specifically in the field of training on how to develop curriculum and provide the training. Again, the NTC has an extensive area for protective forces for the mandated Training Approval Program, and all of the protective forces must meet certain training requirements. DOE assesses these training programs on a periodic basis.

In addition to that training, they offer a full complement of training on the core elements of security within the DOE complex, such as classes on vulnerability assessments, physical protection, protective force, personnel security, and what is called the survey, analogous to the inspection programs—a local DOE office would conduct a survey whereas headquarters might conduct an inspection, and the site would conduct a self-assessment. They are all analogous and follow the same methodologies. Finally, there are courses on MC&A. Courses include the following:

Vulnerability analysis (VA). These courses cover all aspects of VA. They have a fundamentals course, which is good for anyone in the security business, someone who is not necessarily going to be a VA analyst. Besides some entry level courses, they have courses on some of the computer modeling software that is used throughout the DOE complex.

Physical security. These courses cover the Design and Evaluation Process Outline, including all aspects of physical security systems: design, installation, operation, maintenance, inspection, performance testing, and security systems assessment.

Protective force. This is an extensive area of training that goes into some of the tactics necessary, such as protection strategies developed at the sites, firearms, and operations. Firearms training is done routinely at all of the sites. Employees are required to maintain their qualifications for firearms.

Personnel security. This is germane to other discussions during the workshop. This is actually a DOE program for all people who conduct work related to access approval, such as background investigations, clearances, and the Human Reliability Program as well. Training is conducted at the NTC.

Survey. These are excellent courses for those people who may participate in an inspections program throughout the DOE complex. They often use technical experts from the national laboratories as instructors, and the national laboratories are also required to conduct their own self-assessments and to develop methodologies on how to conduct an inspection. Some of the testing techniques, sampling techniques, and the methodologies of conducting the inspections themselves are covered in these courses.

Nuclear Material Control and Accounting (MC&A). There are multiple disciplines involved in MC&A, both at the entry level and beyond. Some entry level courses are designed to create an awareness and understanding of the nuclear field for people who do not necessarily work in MC&A, but who need to understand nuclear materials and some of the associated concepts.

Overall, in DOE, there is a systematic approach to training and that permeates through all of the domestic as well as the international work. It is a rather universal process of analysis design, development, implantation, and evaluation.

The first aspect of analysis is determining who will be trained and the means of conducting that training. This front-end, analytic work needs to be completed before even starting to expend the funds to develop training. Designing the training itself, formalizing the training process, understanding the objectives of training, understanding the various models that would go into a course and the objectives for each of those models, enabling the objectives and incorporating practical exercises, laboratory work, and so forth, depends on the type of course being taught.

Next, one must develop the training material itself. Even those who have developed material, especially for international courses, may have to go through several iterations of the materials. It is always best to have a pilot delivery of the course once it is completed. Courses are constantly evaluated as they are developed into regularly implemented courses. Observers and students should also evaluate the class to provide feedback as it is being implemented. At the end of the course, O'Brien said, it should be formally evaluated again, getting feedback from the students and others involved in the course. Another aspect of many of the courses developed by the DOE complex is special software applications. Technical support is needed after the students take the course so that they have some contact with the instructors or someone who can provide assistance when they actually try to apply the knowledge that they attained.

O'Brien transitioned to international training, having provided the domestic backdrop for training. Through the last several decades, cooperation with

various countries has continued to evolve. NNSA has an extensive program of reaching out and conducting training, sometimes jointly with various entities, sometimes in partnership with the U.S. State Department, and sometimes in partnership with the IAEA.

Often cooperation starts with a technical exchange in a forum such as this workshop where ideas and methodologies are exchanged, and common ground is identified. This exchange is generally followed by a technical workshop, where more detail is discussed on agreed subjects. If there is a joint desire to develop training in a joint manner, then the parties go forward with a training needs assessment and the development of actual formal training. Technical workshops come in any variety of shapes and sizes. Often they are one week in duration, sometimes two weeks. They cover all of the various aspects of nuclear security. Examples include technical workshops on protective force tactics, inspection methodologies, radiation portal monitoring, secure transportation, and VA software tools. It is a very rewarding experience for both entities as they progress down the path and identify common ground on where it is possible to advance technologies in the field of security. The point is that this cooperation is joint cooperation that could lead to formal training in any number of ways. If the cooperation is bilateral, a training course could be held in each country, for example. There could be a composite number of students, either from the United States or from the other country, but it can be done in any number of ways.

Examples of training cooperation from the past few decades include those on VAs, insider analysis, nuclear material monitors, secure transportation, configuration management, physical protection systems, physical protection system performance testing, protective force performance testing, inspections, and security culture. Vulnerability assessment training has always been a keen interest over all the years of cooperation. More recently there has been more emphasis on insiders, leading to the development of actual insider courses, aside from general VA courses. Even secure transportation-type VA courses have been developed. Nuclear material monitors of all shapes and sizes, such as special nuclear material portal monitors have also been discussed in training courses.

Configuration management is something that has been more recently developed, and that deals with the management aspects of maintaining proper configuration over systems, managing change in operational facilities and how to conduct that change while maintaining the integrity of security. Physical protection systems dealing in general with technologies and performance testing is another example. Performance assurance programs and the means to test systems to assure consistent effectiveness are also provided. Protective force performance training is also of interest. Some of these courses have not been conducted in the partner country, but people from the partner country have actually traveled to the NTC and been trained there. Training could also be conducted at any of the U.S. national laboratories that are participating in the cooperation.

Finally, domestic inspection issues, meaning oversight inspections that a government agency would conduct at the sites to provide effective oversight, and security culture issues, also come in all different shapes and sizes. If one

approaches all of these things properly, good security culture will be instilled, but it does not hurt to add some awareness activities as well.

O'Brien summarized by stating that he hoped that he had provided a helpful overview of how DOE approaches training domestically, and how training is designed and has evolved into some of the international cooperative efforts that the U.S. undertakes with partners. He stated that he truly believes that the pathway to success in any cooperation is in training because it is a very common element for all of us.

DISCUSSION

V.S. Ramamurthy, asked if it would be a good idea for security personnel to be licensed only by the facility they serve. Another asked if something happens at a plant, what should be the response in the public domain? Would that be undertaken by a totally different agency, or does the VA or design basis threat provide some kind of an input for the emergency response as well?

Previously in the workshop, there was an inquiry as to whether or not a conventional bomb attack would be assessed with radiation detectors to check if there is any radioactive material laced with a chemical explosive. The training capability exists but is it then routinely used or is it used only if someone asks for that particular assistance? Who provides the assistance and in what context would they ask for assistance? How would these questions be addressed from the American side?

Regarding the GCNEP, a participant noted that there are several global centers of excellence being established around the world. Is the GCNEP envisioned as a Global/Asian Centre? Who is envisioned as attending besides Indians? Who will be the student body and the instructor body of the GCNEP? How global will it be in terms of the actual participants and contributors to the Centre?

A workshop participant replied that India has entered into a cooperative agreement with the United States and with the IAEA and other countries like France, Russia, and the United Kingdom, so they will endeavor to cater to the regional audience and to regional countries as well as to make it a Centre for particular issues such as health care on a case-by-case basis. But the formal educational program as of today has not been initiated. It will take some time to determine how this formal education program will be implemented and who will be the student body, but most probably it will be established under the HBNI. For this a global audience and a global presence will be sought. With regard to the student body, it will not be large, but topical experts in the respective fields will be invited as instructors drawn from within the country as well as from other countries.

A workshop participant noted that "seismic monitoring" was listed as part of the security module. What is the relevance of this topic? Another workshop participant replied that seismic monitoring is relevant from the point of view of nuclear security event detection.

Phillip Gibbs noted that one of the emerging issues in the last couple of years seems to be measurement control methodology and statistical methods in MC&A. Kumar's presentation listed MC&A, but it did not specify measurement systems, methodology, or statistical methods. Gibbs asked how this topic is covered in this environment.

Kumar replied that there is a training program for MC&A. There was a group operating in the 1970s for nuclear material accounting and control at the facilities. There are now two, the one listed in the presentation and one for DAE-controlled and IAEA facilities. With regard to IAEA facilities, samples were previously analyzed there as well as by IAEA. They also had to have international inter-comparison experiments. In 1972, samples from two reactors were analyzed, but this is no longer being done. MC&A is being done with respect to nuclear material like plutonium and uranium. It is being done by nuclear scientists, both in BARC as well as at Kalpakkam.

A participant asked whether CISF is largely responsible for the physical protection of the nuclear facilities in India. Kumar replied that most of India's civilian nuclear facilities are guarded by Central Industrial Security Force (CISF). The participant then replied that unfortunately the recruiting pattern of CISF or the allure in the ranks of the CISF are not very technology-oriented, and nuclear security requires a great deal of technical capability. In this regard, he asked whether CISF personnel are trained after two and a half years, and then moved on only to have to train some other personnel? Why can't one create a specialized nuclear security force since many more civilian nuclear power plants are going to emerge independently?

Kumar responded that there is a special police force which has been selected from the lower rank personnel of CISF to form a separate category of people trained for deployment in DAE installations. This is not a formal agreement, but typically they will be there for at least 10 years, although not at one installation. They will be rotated among the nuclear installations. So there is a move toward making such policies. He speculated that perhaps an agreement should be reached and more stringent requirements should be established.

A workshop about sensors for dirty bombs. The development of explosives sensors for dirty bombs has already been done and this could go farther.

A workshop participant noted that the Centre is an impressive, very ambitious undertaking and asked whether the funding to create this Centre is at adequate levels per the organization laid out. And, second, how many staff are envisioned to run the Centre in its final form?

Kumar replied that, yes, it is totally funded by the Government of India, and it comes under the current, 12th Five Year Plan Project. The construction site has already been selected and procured, and construction activity has already started. The first level of construction is already complete and DAE is confident that we will be able to complete it entirely. The second question was about the staffing. Initially, the staff will be from DAE. Experts from various institutions, BARC, Mumbai, Kalpakkam, or other institutions will hold joint positions, and it is expected that once the institution becomes operational at its

site near Gurgaon in Haryana, initial staffing will be on the order of 100, which will subsequently increase to 250 or 300. This is the projection given to the Government of India.

A workshop participant responded to the comment about CISF security. First, 90 percent of security at nuclear establishments is no different from any other sensitive industrial installation. The only difference is the radioactive material inside the nuclear establishment. CISF essentially addresses access control. CISF forces are given very clear instructions regarding who is to leave, how they are to leave, and what kind of card they have to see to allow them to leave. Many of them are graduates. One would be very surprised given the employment position in this country. They are quite intelligent and aware of what they need to do. One cannot expect them to know the difference between uranium-235 and plutonium-239, but this is not needed. Second, beyond access control, the rest of security has to be conducted by intelligence or red alerts, at which time the higher echelons of the atomic energy establishment as well as the security in Delhi and in the state come into the picture.

A workshop participant continued this discussion by adding that there is a level of induction for the CISF staff specific to a nuclear installation at the level of entry. Retraining is also conducted. What CISF is directly responsible for what is known in the United States as weapon qualification criteria. CISF reports to the Ministry of Home Affairs, therefore DAE has no role except that CISF depends on their own institute for the training and retraining mechanisms and for their qualification. There is also a very good training institute in Hyderabad**.** They are also trained on electronic systems and gadgets and their performance levels are increasing. They are very bright students.

6

The Emerging Science of Nuclear Forensics

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- There are strong scientific capabilities in nuclear forensic science but our ability to interpret these data is still in a state of development.
- Expanded databases with information on nuclear material around the world are needed.
- Greater understanding of how materials change as they undergo reprocessing, processing and other processes is needed.
- No single technique provides the needed information for all or even any material.
- Nonproliferation nuclear forensics requires a focused international cooperative effort.

Promising Topics for Cooperation Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions are not those representing the consensus of the participants, but are rather a selection of those topics offered by individual participants throughout the presentations and discussions.

- Development of national nuclear forensics libraries.
- Sharing of best practices.

- Detection and age-assessment of uranium and plutonium in environmental matrices.
- Cooperation through the International Atomic Energy Agency (IAEA) and the International Technical Working Group Round Robins.

An Emerging and Still Inexact Science

Ian Hutcheon gave an overview of nuclear forensic analysis as it is practiced in the United States and some examples of different types of applications, particularly with regard to the international arena and what is sometimes called nonproliferation nuclear forensics.

Nuclear forensics is the technical means by which nuclear materials are characterized. It is an emerging science because even though nuclear forensic analysis was first applied in the United States in 1949 to diagnose the first Russian nuclear explosion, nuclear forensic analysis as we apply it today really began only in the mid 1990's, and in an international context it has really been applied only within the past 10 years. It is an imperfect science because even though analysts can use sophisticated analytical equipment to characterize material such as interdicted highly enriched uranium (HEU), they often lack the knowledge to identify fingerprints that will allow for the identification of perpetrators and put them in jail.

Weapons-useable material today is found in at least 40 different countries. Because the threats of nuclear proliferation and nuclear terrorism rise above all others, methods are needed to prevent illicit trafficking of this material throughout these 40 different countries. International safeguards and nuclear forensics must work together to make sure that these materials remain under lawful control and in the event that illicit trafficking does occur, the perpetrators are rapidly identified. Meeting the threat of nuclear nonproliferation is a critical 21st century issue that no single country can hope to solve independently; it requires global cooperation.

Figure 6-1 is a timeline of seizures of weapon-useable material going back to 1992. It differs from the IAEA illicit trafficking database in that it contains only HEU and plutonium. There were a large number of events in the early 1990's associated with the fall of the Soviet Union. What is particularly troubling is that nuclear material continues to be smuggled: interdictions occurred in 2001, 2003, 2006, 2010, and even in 2012. Altogether, this interdicted material amounts to about 15 kilograms of HEU and about 400 grams of plutonium. In itself, this is not enough to make a weapon, but these are only the cases of successful interdiction. If the drug trade is indicative of our success rate for interdiction, this could be as little as 10 percent of the total amount of material being trafficked.

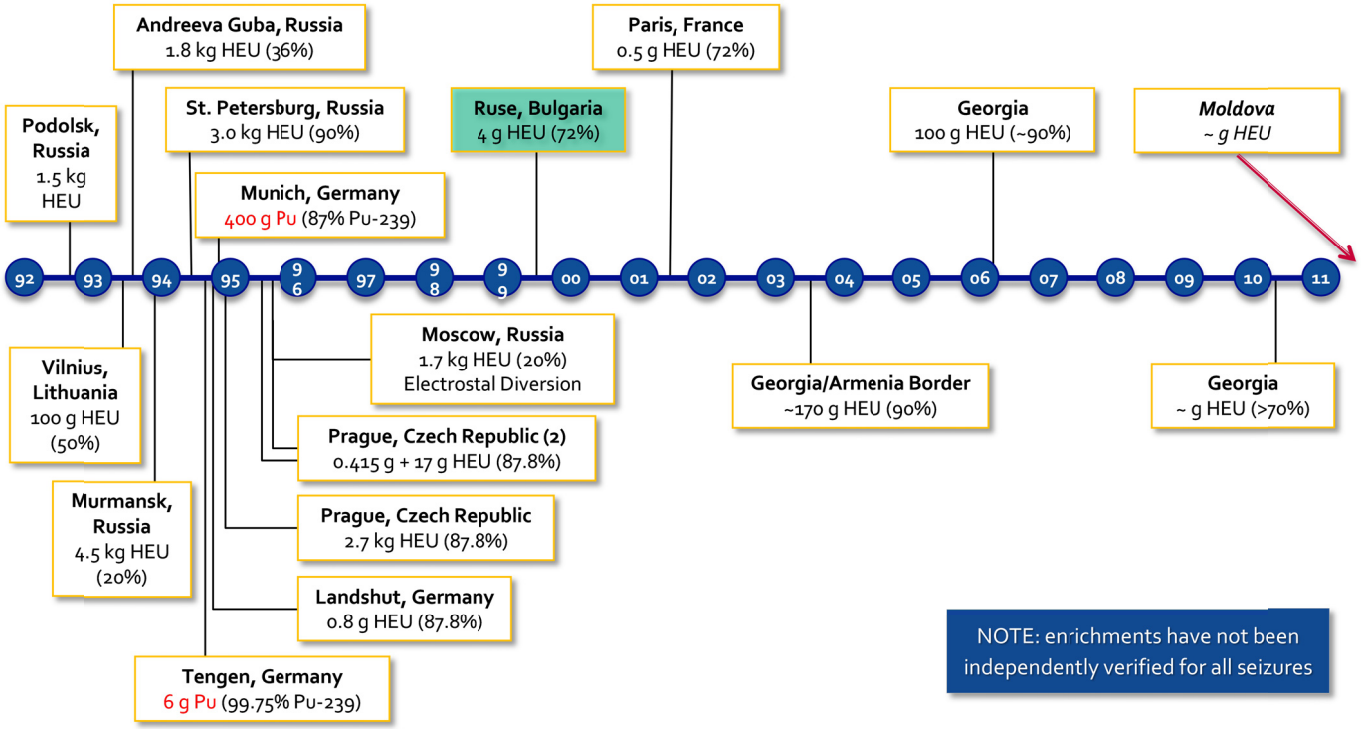

FIGURE 6-1 Interdictions of weapons grade material from 1992 to 2012. SOURCE: Hutcheon, 2012.

After using analytical techniques to characterize nuclear material by its isotopic composition, major and trace elements, its microstructure, morphology, and age, an evaluation process begins. In rare cases, a subject-matter expert may recognize what the material is. In most cases, evaluators have to compare the characterization with material in a database or with some information about the process history to reach technical conclusions; most importantly, who is responsible. Work is needed to improve in this area of reaching technical conclusions based on fairly sophisticated signature analyses.

Signatures are created and destroyed throughout the nuclear fuel cycle. The key for nuclear forensics is to understand how these signatures are created and how they are modified so that if material from the back end of the nuclear fuel cycle is interdicted, the history can be reconstructed and can help to identify where the material was taken from lawful use. But there is no silver bullet: No single signature identifies nuclear material. Figure 6-2 is a Venn diagram that shows that nuclear forensics succeeds by finding the point of intersection between many of these different signatures, including both nuclear and traditional signatures like packaging, fingerprints, hairs, and fibers, and in lucky cases there is a single point of intersection that leads back to the perpetrators.

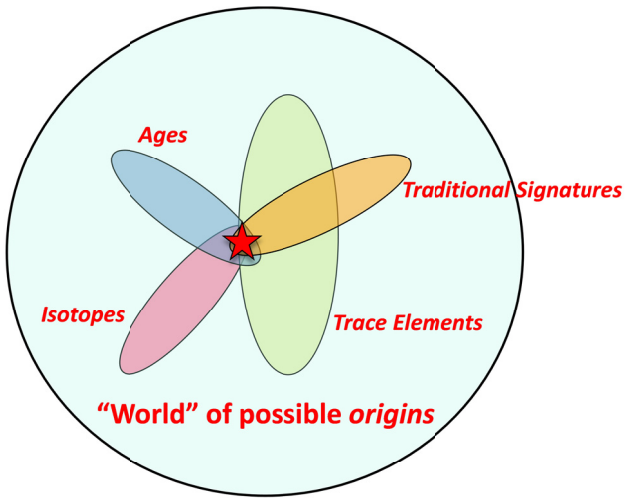

FIGURE 6-2 Conceptual illustration of nuclear forensic characteristics and the domain of possible material that matches those material characteristics. SOURCE: Hutcheon, 2012.

Hutcheon described three different ways of applying nuclear forensics: point-to-population comparisons, which are used to connect a forensic sample to a known population of materials, such as uranium ore concentrate from a particular mine; point-to-point comparisons, which are useful if trying to match material to a specific source or two samples to the same source; and point-to-model comparisons, which are used to explore the possibility of origins for which comparison samples are not available or databases are inadequate. An example of each of these is listed below.

Point-to-population comparison

Uranium ore concentrate or yellowcake is the final product of uranium mining and milling and it is a fungible commodity with worldwide regulated trade. It is a good example for nuclear forensic analysis in part because it is relatively signature rich. That is, it comes in a variety of chemical forms and many chemical and isotopic characteristics vary based on the origin of the product. Yellowcake ranges anywhere from about 50 percent uranium to 80 percent uranium. The remainder is made up of elements which can be measured.

The U.S. Department of Energy (DOE) and three national laboratories (Los Alamos, Livermore, and Oak Ridge) have constructed the uranium sourcing database and library, which consists of about 300 physical samples of uranium ore concentrate or yellowcake from around the world and a larger database containing data on trace elements, isotopes, and physical characteristics for more than 4,000 samples. When a sample of yellowcake from an unknown origin is analyzed, the results can be fed into a statistical algorithm that compares the results to the entries in the database and finds the most likely matches to the unknown sample. This approach works with about 90 percent accuracy today.

Point-to-point comparison

Two samples of HEU were interdicted, one in Bulgaria in 1999 and the other in Paris in 2001. Both are black; both are uranium oxide; and both were found in glass ampoules. Are these two samples from the same source? This is a direct point-to-point comparison. It turned out that the answer is yes, and this was determined by comparison of results from similar analyses by the DOE and the French Commissariat à l'énergie Atomique: uranium isotopic composition, trace elements, determined material production age, and estimated irradiation history of the sample. There is a match for each characteristic, so both organizations independently concluded that the two samples represent material from the same production batch in the former Soviet Union, circa in the early 1990's.

It turns out that these two samples were also contained in lead containers that looked remarkably similar. Both containers have distinctive yellow wax liners, and it turns out that both the yellow wax and the lead are remarkably similar between these two containers. So evidence from both the nuclear material

and the associated non-nuclear material indicate that these two samples were from the same source and were probably trafficked across Europe to find buyers by the same or closely related organizations.

Point-to-Model Comparison

In this case, the analyst may be evaluating what kind of reactor a sample may have gone through. The ratios of uranium isotopes in a sample vary based on the original enrichment of the fuel, the neutron spectrum of the reactor, and the length or irradiation; together these properties can reveal the reactor type.

Hutcheon concluded by saying that nuclear forensics has highly developed technology and can analyze samples ranging in size from kilograms down to picograms with high accuracy. However, our ability to interpret these data is still in a state of development and there is really no substitute for building expanded databases with information on nuclear materials around the world. Nonproliferation nuclear forensics requires a focused international effort. No single country can take this on alone and international engagement on nuclear forensics supports agreed international efforts to counter nuclear terrorism as discussed, such as the Global Initiative to Counter Nuclear Terrorism (GICNT) and United Nations Security Council Resolution 1540. This is an important problem requiring the best science. Connecting cutting edge science to nuclear forensics attracts the best and the brightest scientists, which is how nuclear forensic science will continue to progress.

Nuclear Forensics and Special Nuclear Materials: An Indian Perspective

V. Venugopal defined nuclear forensics, described many of the techniques of nuclear forensics, and explained its value using two case studies. Venugopal noted the multitude of definitions in use for nuclear forensics, but presented this one as his preferred definition:

> Nuclear forensics is the technical means by which nuclear and other radioactive materials, whether intercepted intact or retrieved from post-explosion debris, are characterized as to the composition, physical condition, age, prevalence, history, and interpreted as to the provenance, industrial history, and implications for nuclear device design, etc.

Setting aside medical and industrial radiation sources because they were discussed by another presenter, Venugopal focused on fissile material or special nuclear materials (uranium-233, uranium-235, plutonium-239, plutonium-241), which can be used in making a nuclear weapon.

Nuclear forensics techniques are practiced in different contexts in India, such as analysis of nuclear fuel samples from reactor cores and radioanalytic support for India's courts. There is a forensics laboratory in Bhaha Atomic Re-

search Centre (BARC) that assists police in investigations of crimes (gunshot residues, lead poisoning, cyanide poisoning, arsenic poisoning). When there were questions regarding seized items, they were sent to BARC. Venugopal noted that many of the samples contained sand or a resin or tail portions of uranium used as counterbalance; none ever contained uranium that exceeded 0.7% U-235. Doing this work for the Indian courts taught Venugopal that not only must the analyses be done correctly, but the interpretation and communication of the results are critically important because the audiences are not necessarily technically trained. For example, an accused thief might be sent to jail for the rest of his life because of the uranium if the analyst simply reports the numerical results of analysis but not that the uranium is natural uranium or is within the background level.

Nuclear forensics begins with an incident. Materials involved in the incident are sampled and sent to laboratories where measurements are made. The data and observations are compared to nuclear materials data bases, such as the IAEA illicit trafficking data base, the research reactor data base, and others. Other information from the incident is also factored in, and from all this, one determines where the material came from and ultimately improves the security at the facility where it originated.

When a sample arrives at the laboratory, analysts first identify what the material is. The physical form (powder or liquid) might indicate what stage of production the sample is from. The analyses typically begin with nondestructive analysis, using high-resolution gamma spectrometry, to identify the material from signature gamma-ray emissions, and x-ray crystallography to examine the microstructure, sample homogeneity—whether the sample represents single or multicomponent systems—particle morphology and size. Today, secondary ion mass spectrometry (SIMS) is so powerful that one can analyze the isotope composition of, for example, Pu oxide or uranium, whether it is a rod shape or a platelet shape. The shape is a result of the heat treatment that the material has undergone. So one can identify whether single or multiple sources of plutonium oxide are present by using particle morphology and characteristics. Unfortunately, although SIMS is available in India for other materials, India is not able to procure the latest SIMS technology for fissile material characterization. For some samples, especially for bioassay materials (such as determining whether urine samples contain plutonium or uranium) BARC may use fission track analysis to go down to very low levels.

The next step is to look at chemical signatures, including both nuclear (uranium, plutonium, fission products) and non-nuclear elements, some of which may have been used in processing the materials (for example, reducing the actinide oxides to metal), thorium, magnesium, calcium, iodine, sulfur, and acid residues, such as chlorine, fluorine, bromine, nitride, and nitrate; contaminants that are included in the metal from processing like beryllium, fluorine, iron, and silicon; and additives designed to moderate reactivity. Knowledge of the overall material, including the bulk and the composition, helps in figuring out where the sample might have originated.

Destructive analysis, thermal ionization mass spectrometry (TIMS) and high resolution inductively coupled plasma mass spectrometry, gives very precise and accurate measurements of the isotopic composition or mass abundance of uranium, plutonium, and other materials. The isotopic composition can also give indicators of the history and provenance of the material. If uranium contains U-236, we know that it was irradiated in a reactor. If the uranium sample has a higher percentage of U-234 than the natural abundance, that means that the uranium has passed through an enrichment process. The isotopic composition of plutonium tells us the burnup of the fuel in which it was produced and the neutron spectrum (hard or soft) in the reactor where it was produced. Analyzing residual isotopes using chemical processing techniques and fission yields, one can find out krypton and xenon isotopic abundance and figure out on that basis when the object might have been cast.

By looking at the abundance of each material in a radioactive decay chain, one can deduce when the material was irradiated in a reactor or purified. The specific radionuclides used are called isotopic chronometers. For example, cobalt-60 decays to nickel-60. The ratio of cobalt-60 to nickel-60 tells us when this Co-60 was produced. Uranium has several isotopic chronometers. By looking at the decay daughters, one can find out when the uranium was purely separated. Radioactive decay is a built-in chronometer. One can use isotope dilution mass spectrometry, and isotope dilution alpha spectrometry to detect daughter isotopes at ultra-trace levels. For example, in the case of U-233 irradiation, one can identify the U-232 content very precisely and accurately using alpha spectrometry. This is being practiced very routinely in the laboratory.

Thermal ionization mass spectrometry is the mother of all measurements done for isotopic composition, but it is very difficult to acquire these devices. As a result, to analyze nuclear fuel to support nuclear fuel fabricators, BARC had to construct these instruments (i.e., its own TIMS). Venugopal estimates that in terms of precision and accuracy, it may compare to European equipment from about 1995 to 2000. More sophisticated TIMS equipment may be available now from Germany or the United Kingdom.

Detailed analyses of non-nuclear constituents might reveal the geographic location of production or how the sample might have been produced based on the composition. There is a database focused on such non-nuclear constituents. Alloying or cladding materials may also reveal useful information: the presence of gallium suggests that it was used for stabilization of a particular phase of plutonium. The non-nuclear composition can indicate who the producer might be.

Nuclear forensics is a piece of the international effort to combat nuclear terrorism. There are plenty of examples of interdictions of nuclear smuggling, especially in the 1990's. The materials include HEU, Pu, and even enriched lithium. Their signatures are well known, whether irradiated or unirradiated.

There are many techniques available to characterize and report on the material (including glow-discharge mass spectrometry, x-ray fluorescence, gas chromatography-mass spectrometry, and others in addition to those already mentioned). The goal is to do this complete analysis and to report on key parts

of the analyses within specific timelines. For that report, it is important for the scientist to understand not only the science but the way the courts will use the report. Venugopal gave two examples of cases.

Case Study 1: Lauenforde

A confiscated nuclear fuel pellet was analyzed in June 2003. The data are available from the Institute for Transuranium Elements in Germany. The sample was analyzed and, based on the composition and contaminants published in open literature, one can determine where the sample came from. The laboratory subjected the sample to high-resolution gamma spectrometry. It was found to be unirradiated uranium fuel. Destructive analysis showed the uranium content was about 80 percent and using isotope dilution mass spectrometry, wherein the sample solution was spiked with uranium-236 and thorium-233, analysts found the sample to be enriched to about two percent. The constituents were separated and by comparing the abundances of parents and daughters in the uranium decay chain, the age of the uranium was found to be 12.6 years. The analysis was carried out in 2003, so the material was produced by the end of 1990. The impurity composition was also examined. Based on the discovered age, the production time, pellet dimensions, isotopic composition, impurity content, percentage enrichment, analysts compared these to entries in a database at the ITU and found the pellet to be for an RBMK 1300 Russian graphite moderated reactor.[1]

Case Study 2: Munich Airport

In the Munich airport in 1994 on a Lufthansa flight to Moscow, a sample of material was confiscated. It contained mixed oxide powder (uranium and plutonium oxide, or MOX) 560 grams and 210 grams of lithium metal. The sample was 64.9 weight percent plutonium and 21.7 weight percent uranium, and the lithium was highly enriched, 89.4%, in lithium-6. The isotopic composition of the MOX powder was found to include weapon grade uranium and low (1.66 percent) enriched uranium, which would probably be for a naval reactor or something like that. The most important discovery was that there were two distinct forms of plutonium oxide: hexagonal platelets and rods. This implies two different sources of plutonium for this sample. The plutonium was probably from two different lightly irradiated fuels or weapons grade high-burnup fuel with no direct connection with the uranium in the sample. Where the lithium came from is unknown. This case has not been solved.

Venugopal closed by noting that these and other examples illustrate that radioanalytical chemists need to have many kinds of technical skills and have to interpret the data so that they will withstand legal scrutiny.

---

[1]RBMK – *Reaktor Bolshoi Moshchnosti, Kanalnii* or High Power Channel-Type Reactor.

DISCUSSION

In the case of bullet-lead composition, it has been found that there is as much variation within a batch as there was across batches. Hutcheon noted that in nuclear forensics some batches are homogenized by the manufacturer, but some samples are heterogeneous. Indeed, some samples that appear homogeneous on a bulk scale are actually heterogeneous when examined grain by grain using SIMS. This is an area in which more research is clearly needed. We need to understand how trace element or isotope signatures are imparted into different types of nuclear material.

While the focus of the workshop is on fissile material, the question was raised whether nuclear forensics can determine the provenance of radiological sources that are found, interdicted, or used in an incident. Venugopal described analyzing a sealed source of cesium-137 in what turned out to be a moisture density gauge, which was handled without difficulty. He also reiterated that in the case of a source like cobalt-60, the age of the radioactive material since it was purified can be found.

One member of the audience noted experience with the Oklo natural reactor where billions of years ago natural uranium went critical on and off for millennia producing tons of plutonium. Geochemists and other scientists today determined when it happened, how it happened, how frequently it came on and was switched off, and then where the plutonium went. Some of the same analytical techniques used for the Oklo reactor are used for nuclear forensics.

Another audience member noted that the current state of nuclear forensics as an emerging and imperfect science is dangerous. Particularly in India where nearby there are hostile parties who function on the basis of plausible deniability or even implausible deniability, so long as it cannot be proven. This should be a ripe area for international cooperation and particularly a prime area for collaboration between Indian and U.S. scientists with reference to everything we know about India's western neighbors. Venugopal replied that this work requires a very high level of radioanalytical capability, and while there are some courses being conducted, India is unable to obtain some of the most useful state-of-the-art tools for analysis—SIMS and even the latest TIMS equipment—which are needed for analyzing the minimum sample size. If Indian scientists had such equipment, he said, they could do work on par with those of other international scientists.

Hutcheon observed that nuclear forensic science has improved substantially since the Munich seizures in 1994, and concluded that the worldwide community would do a better job today. He also said that scientists in the United States are eager to cooperate in nuclear forensics. IAEA is also encouraging all member states to cooperate on nuclear forensics and the agency offers an annual training course on nuclear forensic analysis. Another participant noted that nuclear forensics was discussed in the preparatory meetings for the 2012 Nuclear Security Summit in Seoul and the GICNT is preparing a document on nuclear forensics, so the topic is now getting the attention it is due.

The question was raised whether the IAEA could put together a comprehensive databank of material that is under IAEA safeguards. Hutcheon explained that the IAEA has adopted a policy whereby it is encouraging countries to develop their own national nuclear forensic libraries, and then to make them available for query in the event of an international incident. Such libraries are actively being developed in the United States, South Africa, Ukraine, the European Union, France, and the United Kingdom. There is not an on-going effort to develop a single database that would be worldwide in coverage.

Finally, an audience member asked how to ensure that natural uranium used for armor penetrating munitions does not cause occupational hazards for those working with the uranium. Several experts answered that the major hazard from depleted uranium is not radiological, but the chemical hazard as a heavy metal. So it should be treated in the same way as any potentially toxic heavy metal. This problem has been analyzed by the defense laboratory at Jodhpur.

7

Nuclear Energy and the Challenge of Development in India

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- India faces many acute challenges of energy development, which has caused the country's leaders to consider India's indigenous energy sources and how it can increase energy supply to better meet the exponentially expanding energy demand.
- Given this demand, India has chosen to pursue nuclear energy as a source of energy, and is planning a rapid expansion of the nuclear power sector in the coming decades.
- Green scenarios (solar, nuclear, or a combination) should be considered.
- Development deficits and lack of sufficient energy are also issues that can create their own security problems over time.
- India has chosen to develop a closed fuel cycle because of its limited domestic sources of uranium.

Promising Topics for Collaboration Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions are not those representing the consensus of the participants, but are rather a selection of those topics offered by individual participants throughout the presentations and discussions.

- New, safer reactor designs are of interest to India and the United States.
- The need for nuclear energy as a component of the overall energy future is uncertain and could be jointly studied.

India faces many acute challenges of energy development, which has caused the country's leaders to consider India's indigenous energy sources and how it can increase energy supply to better meet the exponentially expanding energy demand. Given this demand, India has chosen to pursue nuclear energy as a source of energy, and is planning a rapid expansion of the nuclear power sector in the coming decades. **Anil Kakodkar** delivered a special lecture during the workshop entitled, "Lowering threats in sustainable development using nuclear energy," which highlighted several issues discussed by other presenters and which provided important context for the realities on the ground in India as they relate to the country's energy needs as well as the long-term development of its nuclear energy program. Moderator **Arcot Ramachandran** noted that the energy need is two to three times the global average of 1.7 percent. Coal fossil fuels add more carbon dioxide into the air, but while nuclear energy is carbon-free, there are associated challenges, such as security threats and other risks. With that backdrop, Ramachandran introduced Kakodar, noting that he is a mechanical engineer and former chairman of the Atomic Energy Commission, and was responsible for the design and construction of many of the nuclear reactors in India.

Kakodar began his remarks by stating that from his perspective, the question of nuclear energy is intriguing, given the topic of the workshop itself: technical aspects of civilian nuclear materials security. The proposition Kakodar made is to consider nuclear energy as a solution to the larger problem of security-related risks connected with development assets because nuclear energy is one important means of addressing development issues. Security of all types, including conventional security, should be considered within frameworks such as those of physical security, malevolent acts of different actors, and so forth. Fundamental issues also exist and need to be addressed to move closer to permanent solutions. One of those fundamental issues is the link between the Human Development Index (HDI) and the Per Capita Electricity Consumption (see Figure 7-1).

The circled area in the top left is the optimum region where, if we are able to find that much energy for all citizens of the world, we would have met an important criteria on the HDI. One can look at the world in two parts, one part on the right side of that particular circle, that is a world essentially consisting of industrialized countries where the HDI is unaffected by the change in electricity use. Whether one increases electricity use or decreases electricity use, it is not going to make much difference in terms of the HDI. And then there is another part of the world on the left-hand side of that circle, where the HDI is, in fact, very strongly dependent on access to electricity. There is a larger part of the

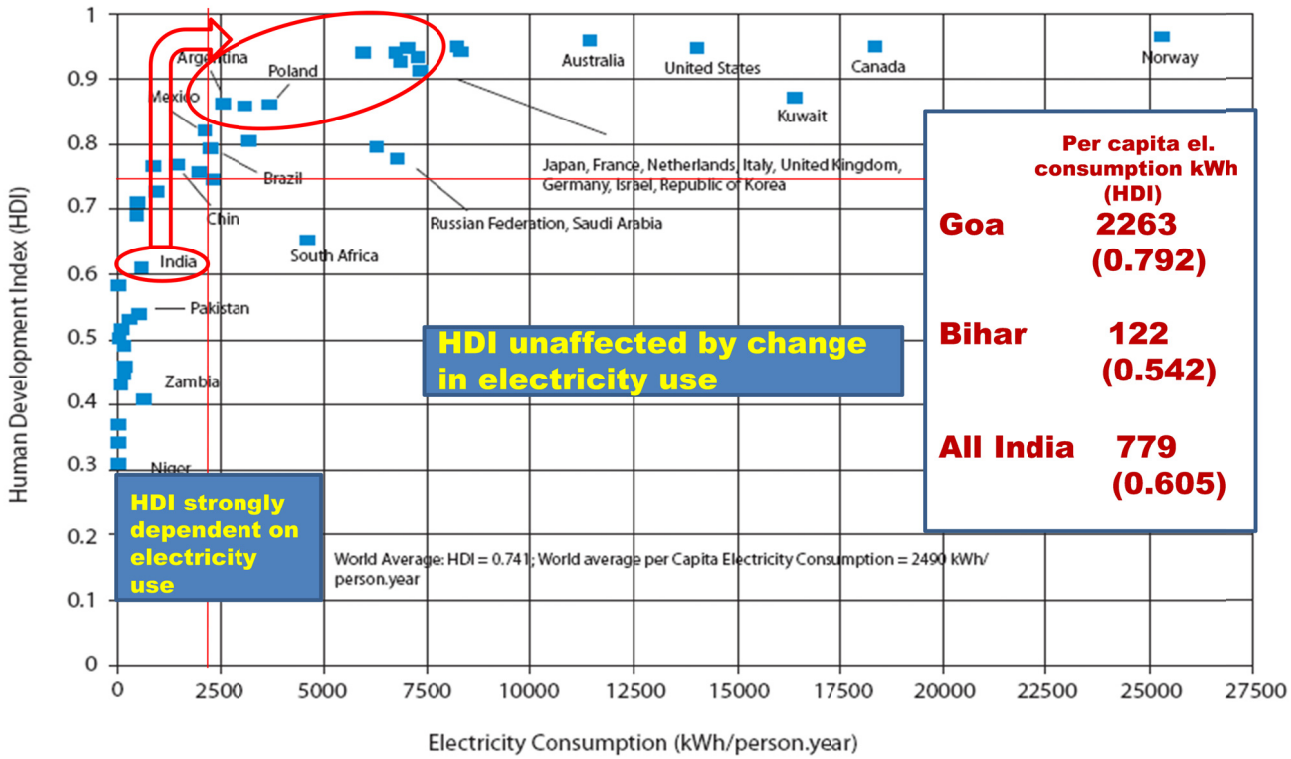

FIGURE 7-1 Human Development Index and the Per Capita Electricity Consumption. SOURCE: Kakodkhar, 2012.

world, the emerging economies like India and China, which are very rapidly moving toward economic growth and they all certainly would require more energy. Moreover, the countries on the left side of the graph make up a large part of the global population, and they are bound to become capable of accessing that energy. They are expected to move to the optimum point (the circle). For example, India is currently at 779 kWh per capita and if this were to increase to 5,000 kWh, one could hope to be able to open at least one important condition necessary to reach the highest possible HDI. Kakodkar noted that the picture across India is varied. The lowest per capita kWh consumption is in Bihar (122 kWh/per capita), and the highest is in Goa (2,263 kWh/per capita). In short, there is a huge demand for electricity that needs to be fed to realize improvement in the HDI in a fairly large part of the world.

The Organisation for Economic Cooperation and Development (OECD) countries represent the industrialized countries with a Gross Domestic Product above a particular threshold. Table 7-1 indicates the population, annual electricity generation, and annual carbon dioxide emissions for OECD and non-OECD countries.

For the per capita kWh usage to increase to 5,000, corresponding to the capacity use attained by industrialized nations, generation of something like 20 trillion kWh would be required. In other words, this would be roughly doubling the amount of energy produced today. Therefore, this is the key development challenge or the key energy challenge. It is also a security challenge because disparity is one of the core issues that leads to conflict and security issues around the world.

Producing 5,000 kWh per capita will take time, therefore it is important to conserve equitable resources for this purpose, because we are living in a world where resource depletion is occurring. Of course there are new resources becoming available, but they are not always available in poorer countries. In this context, energy assurances are important, and this, Kakodar believes, is a prerequisite for long-term peace and security and stability.

TABLE 7-1 Population, annual electricity generation, and annual carbon dioxide emissions for OECD and non-OECD countries.

	OECD Countries	**Non-OECD Countries**	**World**
Population (in billions)	1.18	5.52	6.7
Annual Electricity Generation (trillion kWh)	10.6	8.2	18.8
Carbon Dioxide Emissions (billions of tons/year)	13	17	30

SOURCE: Kakodkar, 2012.

In addition, the threat of climate change requires a reduction in fossil energy use, so this challenge cannot be met in a business-as-usual mode. "Green" scenarios (solar, nuclear, or a combination) should be considered, but every time there is a serious study conducted, precious time is lost. When green energy scenarios are compared with other energy sources, nuclear energy will probably not play a large role. This is due in part to the fact that the world is scared of nuclear safety and security issues, which is reducing investments in nuclear power. On the other hand, can we live with the risk of climate change? When considering the spectrum of green energy sources, inevitably there will be a minimum contribution from nuclear energy if one wants to meet energy requirements.

Next, we must calculate how much uranium would be required to meet a scenario of nuclear power as part of the overall energy supply. For this particular scenario, by 2025 there would not be enough additional uranium to commit to a new nuclear power plant. Depending on the scenario, this may shift to 2035 or 2040, within the next 20 to 25 years there will not be sufficient uranium to move away from fossil fuels to a reasonable extent, particularly when uranium is used in a once-through mode, which is most common today. Again, this depends on the uranium supply, and, of course, just like other resources, more uranium surely would be found in the future. But if we consider the resources and numbers as of today, regardless of what category of resources one is talking about, Kakodkar stated that it is absolutely clear that uranium by itself in a once-though mode cannot supply the total energy requirements on the scale he discussed above. He has stated this at International Atomic Energy Agency (IAEA) meetings, including those where Nuclear Energy Agency (NEA) representatives were present, because IAEA and the NEA said that when they produced their Red Book, they produced estimates of how much uranium is available. Kakodkar received replies of disagreement at those meetings, but when the next Red Book was released, fine print had been added saying that there was sufficient uranium "at the current level of uranium use." This was Kakodkar's point: If uranium use remains at the current level, then the climate change issue is not addressed. If one wants to address the climate change issue, then the issue of the closed nuclear fuel cycle has to be addressed. These are the only two alternatives.

Another issue to consider is spent nuclear fuel. If uranium is used in a once-through mode, the spent fuel has to be disposed of and this is an unresolved issue, and is likely to remain unresolved for a long time. This is because there are legal frameworks that require safeguards, including physical protection. Even if one were to dispose of the spent fuel in a geological repository, safeguards would still legally apply.

Leaving aside the legal issues, if spent fuel is disposed of as spent fuel, it eventually leads to the creation of a plutonium mine over a period of time. Spent fuel is difficult to handle today but it will be easier to reprocess the material in the future when a good portion of the radioactivity has decayed away. This may happen, but not in foreseeable generations. Humanity will be still around, Kakodkar said.

So are we acting in a responsible manner in leaving such a legacy for the next generation? This is why disposal of spent fuel remains an unresolved issue and the only way to handle this issue, Kakodkar stated, is to recycle by removing the uranium and plutonium using technologies currently available. There are, of course, some residual issues in terms of byproducts (actinides, long-life fission products), but there are technologies for disposal of these byproducts, not disposal repository that has to stand geological times, but as complete degradation of radioactive waste in a time span comparable with the institutional lifetime. This technology should be available soon.

This is the approach that we should address from a long-term security perspective, because it is more stable and sustainable, but today, this approach is discouraged, certainly for valid reasons. We discourage it because there is fear of diversion of weapon usable material. In other words, the question of security risk management is a question of the capability of human society to manage this situation. It is important, therefore, to consider the risks in this context. On the nuclear side, there is the risk of diversion of nuclear materials for weapons purposes, that can lead to risk anywhere depending on where the diverted material travels. There is also a risk in terms of threat to the nuclear facility because a breach of security would cause serious public trauma, primarily in the neighborhood of that facility. The risk of diversion can be mitigated by not reprocessing the material so that the weapon-usable material is not freely available. Second, risk can be mitigated by the security architecture in place. On the other hand, the absence of sufficiently large deployments of nuclear energy would make dependence on fossil fuel inevitable. Third, there is the difficulty of predicting global consequences arising from climate change.

But that risk could be much larger than risks posed by weapons of mass destruction. These two issues should be considered together. Development deficits and varying energy security challenges are also issues that could create security problems over time. Kakodkar stated that he believes the need to reduce the risk to humanity necessitates rapid growth of nuclear power. Further, he believes that security measures alone are unlikely to be sufficient. The sovereignty of nations, varying degrees of security as perceived by other nations, responsible behavior or the lack of it, trust deficits, and the need to manage non-state actors are likely to remain difficult challenges. Therefore, the question is how to deal with minimizing the nuclear security risk, while recognizing that nuclear energy should create conditions for rapid growth. This is where technology comes in. Kakodkar is a firm believer that minimizing security risks requires technology; not just technology in terms of physical protection or security architecture solutions, but also technology in terms of the configuration of nuclear power plants, nuclear energy itself.

This is where thorium comes in, which Kakodkar believes is the answer to all of these challenges. It is a one-stop solution to safety, sustainability, and proliferation resistance. If one is concerned about plutonium diversion, once the decision is made to reprocess spent fuel, plutonium can be burned the fastest with thorium matrix fuel, he said (see Figure 7-2).

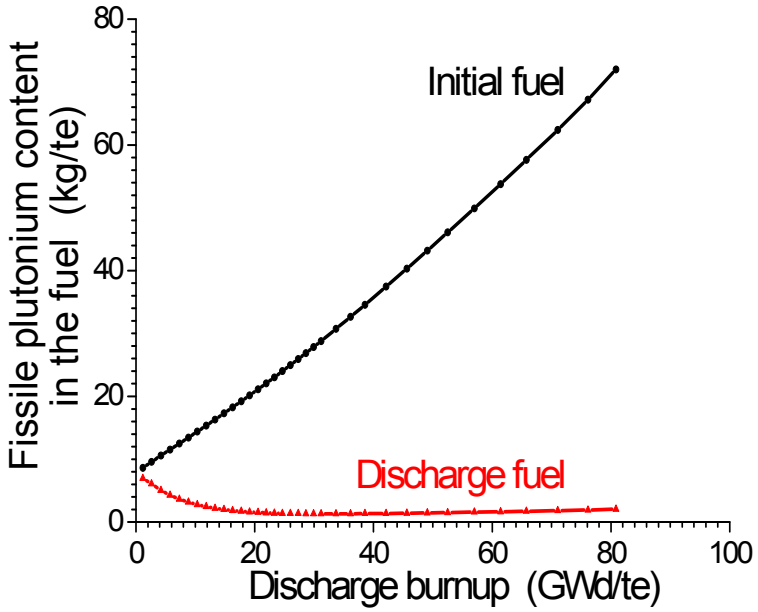

FIGURE 7-2 The plutonium content in fuel at loading and discharge as a function of fuel burnup. SOURCE: Kakodkhar, 2012.

The fissile plutonium content in the irradiated fuel at discharge is low even for low burnup fuel. Furthermore, the plutonium that is produced has a high plutonium-238 fraction, which makes it more proliferation resistant. Uranium-based fuels cannot achieve this reduction because absorption of neutrons in uranium-238 generates additional plutonium. Inert matrix fuel (where plutonium is mixed into an inert material) can burn and degrade plutonium, but one cannot run a reactor loaded only with inert matrix plutonium fuel because the reactor itself becomes unstable.

On the other hand, with thorium, the reactor can run in a very stable manner and degrade plutonium to a very safe level in just one cycle. Uranium-233, which is the fissile counterpart of thorium is present along with a small amount of uranium-232, which is a high energy gamma emitter. While this combination is excellent for production of energy, it has tremendous resistance from diversion, simply because of the lethal dose, which it can give in a short time, depending on the burn-up.

A thorium reactor designed in India, the Advanced Heavy Water Reactors (AHWR), would use 20 percent uranium enriched for 20 percent of the fuel mixed with thorium (80 percent of the fuel). This reactor is not only designed for the normal fuel cycle benefits, but also to attain safety and security advantages. For example, this reactor provides three days' grace period in the event of any accident. This reactor promises no radiological impact on the pub-

lic, even in the event of a severe accident. It has a design life of 100 years and other maintenance advantages, Kakodkar said.

Kakodkar noted that everyone is concerned about the insider threat but he said that the AHWR is designed to guarantee safety against an insider threat. For example, in a scenario where there is a complete station blackout—no power, no station diesels available, and complete failure or deliberate disablement of primary and secondary shutdown systems—the fuel cladding temperature would only rise a small amount, the core would not melt, and there would be no serious accident. That is the worst an insider could do, which provides a degree of immunity even from an insider threat.

A comparable amount of energy is gained from the uranium used in pressurized heavy water reactors and light water reactors, but there are fewer proliferation concerns with thorium reactors.

With thermal reactors, nuclear energy can increase with reduced risk in a variety of new regions in the world. The challenge still remains, however, of meeting energy needs beyond what can be supported by thermal reactors. Fast reactors will still be needed, Kakodkar said, because that is the only way one can increase the energy generation capacity of nuclear power.

Fast reactors and uranium fuel enrichment and recycle technology return us to the question of plutonium diversion. Kakodkar believes that these technologies should be contained within a responsible domain. This does not mean dividing the world into responsible and irresponsible domains. Rather, fast breeder reactors should be implemented in responsible domains, where there are more assurances, to allow for an increase in nuclear power through the use of thorium.

Kakodkar concluded by saying that this is his proposition for the deployment of nuclear energy, which would address both the energy challenge as well as the security challenge. Today's thermal reactors run on either natural or low enriched uranium. This can be enhanced around the world with thorium in thermal reactors. In order to meet the larger energy requirements, beyond what can be supported by thermal reactors, fast breeder reactors will be needed. With reprocessing plants, fast-reactors and recycling, energy capacity will grow. Eventually, both roads can converge. Breeding with thorium in thermal reactors is limited, but advanced reactor systems can breed more effectively to enable growth. He hopes that the world will create an environment that facilities development of nuclear energy that meets energy requirements and security requirements worldwide. If this path is followed, some nuclear security risks will remain, but the world would become a vastly safer place.

DISCUSSION

Raymond Jeanloz began by stating that he was intrigued by Kakodkar's suggestion that for this enhanced deployment of nuclear power, there will have to be a focus on more responsible parties. What organization, what mechanism, what structure would be involved in terms of international organization (in the

cutoff between responsible and irresponsible parties)? Would this be using existing organizations, such as the IAEA, or something entirely separate?

Kakodkar replied by stating that, for example, in Nuclear Suppliers Group-level discussions, there is already movement on how to address the enrichment and reprocessing issue. There are some seeds of that kind already there. He is not in favor of completely dismantling the existing framework. We should be able to build on what is already there, but clearly there are fault lines in the existing framework. Defining what is responsible and what is not is always going to be difficult. Every country will argue that it is responsible. But given the direction in which the discourse is moving, one could make progress.

A workshop participant asked: What data exists on the availability of thorium?

Kakodkar replied that there is plenty of data available and in India, the availability of thorium is much greater than what is currently known or discussed because Indian thorium assessments are based on what has been explored primarily for ilmenite. Some of the ilmenite has been found, and along with that there is so much monazite, which means there is a lot of thorium. He said he would not be surprised if the quantities are in the range of approximately 800,000 or a million tonnes in India, although, thus far much lower numbers have been referenced. There are large-scale deposits in many other countries, including Brazil, Turkey, and the United States. The problem with thorium is that it is available either in countries where there is plenty of uranium so there is no interest in thorium, or in countries where there is no nuclear technology.

S. Gopal asked Kakodkar if he thinks that new discoveries of alternative sources of energy, such as shale gas or hydraulic fracturing, would make OECD countries less enthusiastic about his proposal?

Kakodkar replied that this already happened. The U.S. view of energy sources is quite different from that of India precisely for these reasons, and enthusiasm in nuclear power today has diminished. For example, if one takes the case of Britain when the North Sea resources were found, that actually stopped the nuclear program in Britain. Today, the U.K. is again considering nuclear energy because the North Sea resources have been exhausted. Uranium is not an infinite source of energy and the fact still remains that although oil is better than coal and gas is better than oil, the earth's carrying capacity for greenhouse gas emissions increase daily. How this will evolve, Kakodkar did not know.

Kakodkar was asked what he thought about the promise of nuclear fusion and other new technologies. Kakodkar replied that one cannot compare thorium with fusion in terms of readiness. Although fusion will always need research and new technology, the deployment of thorium reactors can be done on the basis of what we know today. Whereas, with fusion, we have to wait until approximately 2020 for the International Thermonuclear Experimental Reactor to be completed and then one will have to allow for the 15 year time period to conduct experiments to understand the performance of the steady state plasma. So in 2035, construction of a reactor may begin to demonstrate energy production, which will be another 15 years after 2035. If everything goes well, we will light a

lightbulb using fusion energy in the year 2050, and only then can commercial deployment follow. If one really looks at this from the climate change point of view, there is not that much time.

A workshop participant raised the question of solar energy, referencing a recent news item that Germany had a breakthrough and approximately 40 to 50 percent of their energy requirement is met by solar energy. Kakodkar replied that this would be a great development for India. There is a very justifiable, strong emphasis on solar energy in India. There are only two energy resources that India has that met India's needs: thorium and solar. But the question is not thorium or solar because India needs both. Storage of solar energy on that scale is impossible purely from an economic perspective, and one should not put all of one's eggs in the same basket, but have a reasonable portfolio. India does not have much choice: thorium and solar are actually a very narrow range of options. Solar energy is a great development, and India should move in that direction.

A participant asked about lifecycle greenhouse-gas emissions. Thorium reactors do not produce emissions in the production of power, but all that goes into producing a nuclear power plant from beginning to end adds rather than subtracts greenhouse gases. Is there any basis to this?

Kakodkar replied that in fact there are IAEA documents on this issue, where they have looked at the lifecycle emissions from all energy technologies including nuclear, and nuclear energy is actually quite low. In fact, it is lower than hydroelectric power and actually comparable to solar; sometimes slightly lower than solar and sometimes slightly higher than solar. In terms of carbon dioxide emission nuclear energy is very good.

A participant asked about underground nuclear reactors, for which Toshiba has been an enthusiastic advocate. There are underground nuclear power plants in existence. In Switzerland, they are talking about such power plants, not so much due to safety considerations, but because they do not want to spoil the landscape, so they felt that locating a power plant completely underground is a good idea.

This is ultimately a question of cost, and Kakodkar does not believe that by locating a nuclear power plant underground all aspects of safety are fully addressed. One can address the question of an external military attack, certainly an underground power plant would probably do a little better, but with present day or maybe future bunker busters, this may no longer be valid. As far as radioactive releases are concerned, the question is whether there could be failures in the ventilation system and the isolation system. It is not as if with an underground power plant, radioactive emissions could be completely eliminated.

A workshop participant asked Kakodkar about his view of solar energy potential. He replied that in India, if one takes the barren uncultivable land and diverts only 25 percent of it to solar energy, enough energy will be collected to fuel the entire country's energy requirements. Land is not an issue as far as solar

power is concerned. However, he does not agree with the comparisons that have been made for land use in a recent paper in *Current Science*.[1] The comparison of land requirements for solar and nuclear energy should do so without including the exclusion radius because it is not really diverted for any other use. It is still available for deploying solar energy, for example. Co-location of solar and nuclear plants feeding the energy into the cycle is very much a feasible proposition.

Another workshop participant noted that in his presentation, Kakodkar addressed nuclear safety and climate change as two different risks, but the examples of the accident in Fukushima, Super Storm Sandy, or the incident at a nuclear plant in the United States, indicate that more dependence on nuclear energy actually makes the risks from climate change more severe. Moving away from the nuclear energy makes the handling of climate change easier. Kakodkar replied that he does not understand this proposition at all. By climate change one means the warming that will take place because of carbon dioxide emission causing erratic and severe climatic conditions, but a tsunami is not one of them. Tsunamis do not take place because of nuclear power, nor do they take place because of increasing carbon dioxide. They originate in geoseismic conditions. If there were a nuclear accident, a lot of people would have to be relocated, just as in Three Mile Island and Chernobyl and Fukushima. A more balanced approach is needed in terms of deciding appropriate intervention levels when it comes to displacement of people. Although there was radioactivity released, and there was increase in the environmental radioactivity because of reactor failure. Kakodkar said that he does not expect any significant health consequences in the case of Fukushima. After the Chernobyl accident, there were health consequences, but they are much lower than predicted on the basis of the Linear No-Threshold hypothesis. There has to be balance in considering these radiation-exposure risks versus the health costs associated with public trauma and displacement of the affected populations. Over-conservatism in the case of managing accidents does not work.

[1]S. P. Sukhatme (2012) Can India's future needs of electricity be met by renewable energy sources? A revised assessment, *Current Science*, 103(10):1153. Available at http://www.currentscience.ac.in/Volumes/103/10/1153.pdf, Accessed September 3, 2013.

8

Implementing Systems Approaches to Security at Civilian Nuclear Facilities

Key Issues

The key issues noted here are some of those raised by individual workshop participants, and do not in any way indicate consensus of workshop participants overall.

- Security is a national responsibility but has international dimensions.
- Communication with the public is important because in an accident or disaster scenario, there is not time to really explain thoroughly.
- Decision making in an unexpected emergency scenario would involve multiple players: political leaders, operators, regulators, bureaucrats, politicians, representatives of the local community and others.
- The balance between research and security interests is at times difficult to define and maintain.

Promising Topics for Collaboration Arising from the Presentations and Discussions

These promising topics for collaboration arising from the presentations and discussions do not reflect a consensus of the participants, but are rather a selection of those topics offered by individual participants throughout the presentations and discussions.

- Improving the accuracy of measurements may be an area of possible cooperation.
- Jointly discussing risk-based versus risk-informed decisions would be of interest.

- Bringing in experts from other fields to discuss training in dangerous, high-consequence areas, such as aviation, could be of joint value and interest.

Jointly discussing how to incorporate culture into nuclear security issues would be of benefit to experts from India and the United States.

Baldev Raj began by observing that security has become a key word in people's discussions. We talk about an idea of security: food security, water security, and nuclear security. What do we mean when we talk about this word security? We mean that we have concerns, and we know that the concerns are not short-lived, and we have to take systematic approaches: Science, technology, policies and implementation to ensure that various types of security are achieved sustainably.

The risks and the security efforts against those risks are national responsibilities, but they have international dimensions due to connectivity. Consequently, countries have responsibilities vis-à-vis international organizations, and we in the international community study the situation and countries' responses during catastrophes.

Nuclear security includes safety, protection, and nonproliferation. These three pillars are few in number, but the interfaces among them are huge and multidisciplinary, particularly with respect to science and technology. The number of emergencies is increasing, but the maturity in handling these emergencies is increasing at varying rates. Most safety scenarios in today's facilities develop slowly, whereas security scenarios often develop quickly in unpredictable ways, but safety and security are still interconnected. Nuclear safety can be discussed with complete transparency, but the moment the word 'security' is introduced, various levels of opaqueness appear. Because one can speak more transparently about nuclear safety, the maturity of science and technology is much greater, as is the ease of making decisions. This does not mean that one is easier than the other, but there are differences with regard to how much money has been invested, when the programs started, how many people work in which areas, and which analytical tools (e.g., simulation and modeling tools) are available.

The problems are complex. These complexities include a diversity of sources and scenarios. Sources vary from reactors to fabrication facilities to reprocessing to fissile materials during transportation. In the security domain, sometimes responsible parties cannot be transparent. Access in knowledge in databases is provided on an "as and when by whom basis." In nuclear security, the organizations remain, but the repository of information is with the individual people; they are very different and that is important to decision making. Decision making roles are clear, as they are among people, regulators, bureaucrats, and politicians. Raj is not worried much about sources. He is more worried about gaps in decision making in nuclear security. Rogue countries and their operations, conservative and clear versus bold and realistic. This is always a thin line, but often one needs bold, but realistic decisions; being conservative in this case will not work.

The anticipation of human resources, with different expertise and abilities, and communication at different levels with effectiveness and credibility looks so benign that it has been ignored. All of us think that we are very good communicators, and we all know what poor communicators we are. Communication in the nuclear area, particularly in the case of catastrophes or severe accidents, has never been good. Paradigm changes are needed. Perhaps young people who know how to communicate better and very clearly in a short time can help. Younger people should be on committees, and we should be listening to them. Understanding the interface between people and technology is always difficult, but it must be managed. If we don't manage it, we are not going to have a systems approach, we will have a domain approach, which is not going to be successful. Therefore, a paradigm shift is needed.

Raj then noted that lessons learned about nuclear security from one accident in a country cannot be directly translated to another country due to differences between cultures and the way decisions are made. If one were to try to simulate a Fukushima-type accident in China, the United States, or in Europe, there would be different responses in each country, although the science and technology are very similar. Translating International Atomic Energy Agency (IAEA) guidance into different cultures so that it affects how vital decisions are made is difficult.

This gets back to effective communication to educate and enhance the ability to discern between essentials and nonessentials; this is key to solving problems. Take the case of Fukushima. Radiation levels in residential areas may be reasonably low, after decontamination, radiation levels can be brought to completely acceptable levels. With more effective communication, citizens could be involved in the science and technology to conduct decontamination or rehabilitation in a much better way. We keep on talking about microsieverts, millisieverts. Who understands that? Communication with the public has to be very different. These issues need to be well understood by people because in a disaster or accident scenario there is no time to really teach people what to do, unless they were prepared well in advance.

Decision making in an unexpected emergency situation would involve multiple players, each with their own expertise and motivations: very powerful individuals (prime ministers and presidents), operators, regulators, bureaucrats, politicians, representatives of the local community, and others. How, Raj asked, do people who have different knowledge bases make decisions? This must be determined in advance; it could not be determined at the time of an incident because there would be so much confusion and clutter that it would be difficult to identify a small signal among a whole lot of noise in order to make a good decision.

This was one lesson of the Fukushima accident. Decision making regarding response requires an agreement on approach, and implementation, and this is part of a systems approach, stated Raj.

With nuclear security and nuclear safety, there are differences in potential damage assessments with different disaster scenarios. A sophisticated attack on

a nuclear facility could jeopardize both nuclear safety and security. One needs to consider differences in modeling and simulation, advanced sensors, robotics, and instrumentation. Responding to safety and security incidents may present conflicting challenges. One may wish to limit human response where the risks to responders may be deemed very high, yet there may be no other choice, such as in responding to a fire in areas of high radiation concentration. There may be a way to optimize response if good thinking goes into the development of response scenarios that incorporate advanced science and technology. The STAR Project of the European Commission is a good beginning.

Raj noted that the IAEA will also have a central role to play, along with other multinational organizations, and individual countries that offer assistance. Each player would bring very different kinds of cooperation and collaboration, and managing these interactions is very important.

Science and technology must play a central role, be it through modeling and simulation, or be it through decontamination and rehabilitation. Wonderful technologies have been developed in Japan to decontaminate and rehabilitate very large areas, and these would be useful to the world. Robotics are bringing advances in the form of miniaturization and the availability of technologies to all countries, although there are export control limitations. Perhaps where nuclear safety and security are concerned, key technologies could be made available.

A paradigm shift will require that every country do a lot of work to ensure fresh ideas and fresh thinking to move forward and to continue to question each other to make and sustain changes. In this regard, international collaborations have a significant role to play. Raj noted the fact that these issues have been discussed for years and decades indicates that they are important, relevant, and changing. There is now a demand for incorporating a judicious mix of qualitative and quantitative approaches into modeling and simulation approaches to safety and security. Likewise, there are now many means of data and information retrieval, analog and digital approaches for example, as well as hybrid approaches. Based on greater understanding, it is possible to move forward and to improve technologies.

Human resources are the most important aspect. Knowledge alone is not going to help. There are many knowledgeable people on this planet, we also need wise and ethical leaders who can work at these interfaces and make decisions. Raj expressed his view that these people seem to be disappearing. There is a great deal of optimism, however, because there are very capable people who take these matters seriously and who are committed to finding solutions, such as those at this workshop and at similar gatherings. Strategies have to be found, and Raj looks to Galileo, Faraday, Deming, and Taguchi for inspiration.

Specifically, in the area of measurements, there must be a way to improve because correct measurements are key. No matter how much consideration goes into discussions, measurements in each domain must be accurate. Too often we are satisfied with cataloging measurements taken. The right measurements might not have been taken to allow for cost-effectiveness and optimization. This is important especially at the interfaces and in the design phases. Safety and non-

proliferation aspects must be incorporated in the design phase, even beyond the design basis threat approach to appreciate linkages, to anticipate problems, and to not repeat mistakes. Learning from these mistakes might prevent other catastrophes and mitigate harmful effects in the event of an incident.

Raj concluded by referencing the teachings of Buddha from which he draws optimism: detach, clear, balance, experiment, maintain conviction, pursue, achieve.

Systems Approach from a U.S. Perspective

D.V. Rao opened his presentation with a quotation from Will Rogers that guides his thinking on nuclear security: "It is not what you don't know that hurts you. It is what you think you know, but that ain't so that gets you." In other words, it is not what we don't know that is the problem, because we have a way of solving gaps in knowledge. Rather, there are cases where we are certain we know but we are mistaken. These are the problem because we are not very prepared. Systems analysis and the mathematics that underlay it provide an objective way to analyze gaps and communicate gaps.

There are different types of communication as Raj noted, and this communication is done at different levels. On one level, people are very educated but may not be aware of the details of nuclear engineering necessary to address the gaps. How does one communicate with them and demonstrate that one has done the best one can? That is the key: to have done the best possible to determine the gaps, find a solution to those gaps, and communicate those solutions. There are risks, and they must be shared by all populations; this must also be communicated.

Throughout the presentations, one thing has become very clear, Rao said: nuclear facilities are socio-technical systems. Engineers try to make them an engineered system as much as possible because an engineered system is much easier to manage. The social aspects of these systems are not easy to manage. There are certain expectations about social behavior in democratic institutions or democratic countries. How are these accommodated?

To make it more complex, almost every nuclear facility, even reactors, are complex and unique. Therefore, the way they implement security and safety regimes is a one-of-a-kind system. One does not put it on autopilot. In fact, often automation gives false signals, and false signals give security guards reasons to turn off of the sensors: "Oh, that thing always beeps. I (the security guard) am just not going to do anything. It is probably a rabbit jumping over the Restricted Area." Automation may not do the job that one expects it to do.

A second point is that many of the nuclear facilities have a research and development (R&D) function, be it civilian or in the defense industry. Without R&D it is difficult to recruit very smart people to work at your facilities. Rao then asked, how does one balance research interests against the other two competing interests of materials and information security and transparency?

To try to address nuclear security, Department of Energy national labs have been exploring a variety of modeling and simulation and analysis techniques, including visualization techniques. Together they then form the important tools in developing and designing and creating a system to draw the most from that system. Further, regardless of the techniques, there are no substitutes for policy or regularity regimes. There is guidance from IAEA and from Indian regularity agencies. Some of the regulation is prescriptive, not performance-based. Even with prescriptive guidance, we must understand that (1) regulations are based on certain assumptions, either regarding design basis threats (DBTs) or regarding existing technologies and the limitations of those technologies; and (2) the system should be designed to fail gracefully. In other words, if a system is designed based on a threat in which a person would come with a certain number of guns and a certain amount of explosives, and in reality, a person may have double that, the whole architecture may completely collapse. Graceful failure is the goal, allowing the system to be able to function in defeat.

There is a similar term in mathematics: "epistemic uncertainty," or the "unknown, unknown." Because one does not always know what is not known, sufficient margin is needed, but it is not always clear what a "sufficient" margin is. For example, the Fukushima Diiachi plant was not a badly engineered system, but Rao stated that every nuclear power plant operator has known for a long time, through the mathematics of the probabilistic risk assessment, that a station blackout is a possibility. The probability of a blackout and possible causes have been analyzed in depth. There are new regulations in the United States regarding station blackouts. Engineers also have to deal with how to address potential problems at older plants. When those decisions are made, some mathematical techniques can help identify and build consensus on decisions and risk-acceptance at a national lab or state level.

Physics-based models can also help determine answers to questions such as: "If that much of the process material is going through a line, what types of signatures would one expect?" Modeling and analysis tools are improving, and it should be possible to simulate facilities very accurately with high fidelity. As India demonstrates leadership with the fast breeder reactor program and fuel recycling facilities, some of these methods should be used to set guidance for the rest of the world, working with others, because that guidance does not exist.

With regard to DBT, law enforcement agencies, engineers, and subject matter experts come together and assess what is likely to happen from a threat perspective. In case of a smart insider, or an intelligent adversary, some of these methods break down. And the dynamic flow graph and the logical flow graph are methods designed for these threats. It is important to always look for new techniques and methods by which to fuse data and provide data with some degree of confidence, recognizing that all recommendations have associated uncertainties. Some methods are based on inference, some on forensics, and some on force-on-force modeling descriptions. Rao stated that he prefers the term "risk-informed," rather than "risk-based," because risk is one attribute that informs

decision-making. In this formulation, value is assigned to risk, but value is also given to other aspects as well.

One example of this is called a "multi-attribute utility." In this case, one asks "for that fuel cycle and for that operation within the fuel cycle, are the various attributes that contribute toward security?" Working through issues by asking this question makes decision-making more transparent. One attribute, for example, is material attractiveness. DOE has undertaken a process to bring experts from the three weapons labs together and ask them to establish a more scientifically-defensible approach to defining material attractiveness. This process has been under way for two years and has made progress.

With relevance to the Indian nuclear sector, the material attractiveness of light water reactor material and material attractiveness for a fast-reactor are not the same. They are different because the breeding plutonium vector (isotopic composition) is different. There is also a difference between materials associated with light water reactors and heavy water reactors. Experts in India may undertake a similar process and distill the information for others so that they can evaluate options, for example, for treating spent fuel or separated plutonium. Questions remain for all countries that have plutonium. Experts need to find ways by which to communicate the attractiveness of various materials or the inherent security features of materials.

Communicating these issues beyond the scientific community to policymakers raises different issues. For example, if one has pressurized water reactors with very low burn-up rates built in the 1960's, with spent fuel close to the reactor site, the attractiveness of the materials increases. This may lead to the question: "Should the material be kept there, and, if it is moved, should the fuel cycle be closed?" One can also demonstrate that after 50 years, even the spent plutonium fuel becomes very attractive due to low doses of radiation emitted and low heat, warranting attention. These are the decisions that stem from the development of tools and the resulting analyses conducted in a comprehensive way.

In conclusion, Rao noted that the threat spectrum is a continuum. One has to analyze various threats and assess whether nuclear materials would be attractive targets in particular scenarios. Then, a judgment needs to be made as to the level to which one should protect material, a facility, and so forth. The owner of the facility, together with experts, assesses intrinsic vulnerabilities, intrinsic risks, and operational risk. These assessments are coordinated with intelligence information, local police and others, to reduce the intrinsic risk, or to reduce the operational risk as far as possible from the intrinsic risk.

DISCUSSION

Reflecting on Raj's presentation, the discussion moderator noted that in future meetings, it may be helpful to invite a presenter from Boeing or Airbus because they deal with training across multiple cultures on the same, potentially dangerous technology. There are also some academic studies about how people

from different cultures and societies actually learn to fly jumbo airplanes. They have had a lot of practical experience and it might be useful to hear about the lessons they offer.

An Indian workshop participant emphasized Raj's comments about sensors and robotics. This is one area which has grown in India and abroad. Measuring sensors and modeling are also important. Perhaps this could be a topic for future meetings because the participant said, India is not as strong in the area of sensors and their utilization in multiple areas, whether for protection or guarding consistency.

Micah Lowenthal asked Rao and others about systems analyses for identifying areas of leverage points, but also for establishing probabilities. There are multiple camps that have opinions about these tools. At one extreme, one says, "we don't care about the results, it is really the process of going systematically through and analyzing that is most valuable." The other says that, "we really want the results, and that is what is going to give us our prioritization of how we are going to remedy our systems or design our systems." Where do you come out on that? What would you think is most valuable?

Rao replied that he views risk-informed rather than risk-based approaches to be more effective. The process is more important, bringing in subject-matter experts, including mathematics, brings quantification and rigor that adds another level of learning. Coming together makes a greater difference than the final answer.

The moderator then asked for suggestions of materials that might offer a helpful introduction to the science of risk in addition to the book entitled, *Normal Accidents,* by Charles Perrow.[1] Another participant recommended Scott Sagan's work on nuclear safety.[2]

A participant referred to Raj's inclusion of incorporating culture into nuclear security issues as well as the importance of communicating effectively with the public about acceptable levels of radiation for decontamination. How could Indian and American experts actually start to work on these issues? How do we actually explain to each other that we have an equal amount of knowledge, but that knowledge may be in different fields?

Raj replied he had first-hand experience with this because he was in charge of the tsunami response at Indian nuclear facilities in 2004. After the initial emotional shock, they started putting together people who were knowledgeable about the culture of those engaged in fishing in the area, the culture of the bureaucracy, and the culture of how much information to provide. This is important because in a nuclear scenario if the right information isn't given, one can be held responsible for suppressing information. Conservative information might have been provided in good faith, so Raj chose words very carefully, and

[1]Perrow, Charles. 1999. Normal Accidents: Living with High-Risk Technologies. Princeton: Princeton University Press.

[2]Sagan, Scott Douglas. 1995. The Limits of Safety. Princeton: Princeton University Press.

was bold but realistic. People would advise him to not to say certain things, but he responded, "Let us say that we are watching the facilities, and as of now, there is nothing of concern. We have instrumentation and sensors, and if anything develops, we would have information within a few hours." It is extremely important to have complete, clear information and then distill it. There must be a strategy for being transparent and for effectively dealing with that transparency.

Raj's experience demonstrates that if one can be transparent and convincing, one can cut across different levels of knowledge-based bureaucracy, but one has to be transparent, first of all, even at the cost of losing one's job and having politicians unhappy because what is said is something they may not like. This is candor. And the second key aspect is to effectively involve them in the huge job. If they are not involved, just being nice at the time doesn't help. One does not need nice people at that time; one needs people who become a part of the solution. It is possible to involve all stakeholders. In order to do so, one has to understand what the fishermen and fisherwomen, the small shop keepers, the people in general know of the facilities.

Culture comes after knowledge. If one has knowledge, a way of understanding the culture, and communicating, one can have success. This is a subject that needs much more discussion. Immediately after the tsunami, a wonderful meeting was held at the National Institute for Advanced Studies (NIAS), where all of the people who handled this response were called together to try to study how cultures had influence, how they communicated, and where they were successful. The proceedings of that meeting are available. It may be worthwhile to spend a day on this together.

A participant then provided a minor example from the American case that was only 12 hours old. A spokesman for the New York University Hospital stated that when the backup generators failed the hospital as a result of Superstorm Sandy, newborn babies were carried down the street to transport them to another facility. The interviewer kept on asking the hospital spokesman, "Did the generators fail?" And the spokesman said, "I can't answer that question, can't answer that question." He was afraid of a lawsuit. Basically, in the American system, the spokespersons, especially of private organizations, are worried about the legal system. So in this recent case, he could not admit what everybody knew - the generators had failed.

Paul Nelson then commented that the weights assigned to the different security factors do reflect cultural differences. It is often more difficult than one might think to arrive at a consensus as to what those weights should be, even in the context of a given country or a given state. But one can test the sensitivity of the conclusions relative to those cultural factors; sometimes they may not be quite as sensitive.

Another workshop participant commented that it is not easy to convince people who are going to invest human and financial resources into nuclear safety and security based on validating models with mathematics and a vector.

In response, a participant expressed his strong support for modeling, simulations, and analysis as they are the best tools and technologies.

A workshop participant from the United States agreed that when one is asking someone to invest hundreds of millions of dollars based on a model alone, it is very unlikely that they would be persuaded. However, models are tools, and any good modeler knows that models are inaccurate. But, when that model is used within a small focused area together with analysis from subject matter experts who can propagate uncertainties in a rigorous way, trustworthy answers can be found. Any model informs understanding of what is likely and what is absolutely unlikely, and this is the decision point about risks.

Another participant with many years of experience concurred that transparency is very important and that it stood him in very good stead, although at times, he thought that particular statements may cost him his job. But over time, it builds confidence in what one says and people have supported him, for which he is thankful.

A workshop participant from the United States relayed some of his own professional experiences over the years working internationally. Regarding the importance of people, there is a certain amount of integrity of the models as well as of the individual analysts. Over the years in certain cultures, we have shared experiences and knowledge about how to do these types of analyses. There are examples when an analyst from another country has done the same analysis and come up with different numbers and cannot even explain the difference. Ultimately, the analyst would say, "My guy can't take these numbers to my management, because the results are coming out bad." There has to be integrity in the process of conducting these analyses. A lot of money rests on the results sometimes, and at times, bad news has to be delivered to management to force certain security upgrades to take place. There is a bit of a cultural aspect to understanding how to deliver the results of some of these analyses in an effective way and to maintain integrity in the process as well as integrity as professionals. The human element is a key part of the overall security posture and protection planning and everything.

The moderator suggested that for the next meeting or workshop, we might want to commission some case studies, some from America, some from India, successes and failures in dealing with the public during disasters. Clearly, there have been enough failures and maybe some successes and maybe scholars can produce case studies of these successes and failures and we can then try and analyze why they were such. The roles of science and technology in responses to Hurricane Katrina and the Fukushima accident could be case studies, for example.

A participant followed this suggestion by reflecting that when experts were at the IAEA looking at Fukushima modeling in the very early stages after the tsunami, some would say that they had much better models to be able to predict how the hydrogen would appear. However, when that information was given to IAEA, it never reached the Japanese people and it was not clear how it would have been used if it had been reached. The modeling and simulation done by different groups was widely different. As long as the results converge, it is easy, but results can be so widely different that one needs a benchmark exercise.

That takes a long time and a lot of money. Someone has to invest the resources and involve quality people. This is improving.

A participant from the United States noted that the Sandia MELCOR Model, used in real-time to predict the outcome of the Fukushima accident, actually proved to be fairly accurate because it is rigorous. That particular model was started right after the Three Mile Island accident and various agencies and labs have all contributed to that model at different levels and continuous updates have been made. It seems that India is doing something similar. One has to conduct 2D, 3D experiments, separate effects experiments, combine complex experiments and then start assimilating all of that information back into the model. These experiments need to be conducted over years and decades before one reaches a point where one can have more faith in the model. This is something that needs commitment. If all of these investments are made, the models can be very reliable. One has to avoid simply stating that one model is better than another.

A participant asked about the Indian response to the 2004 tsunami. The response seems to have been positive because the individual in charge at that time had the sensitivity and the experience, and perhaps had the wisdom, but did he have formal education and training? This has to be part of a senior leader's background (deputy heads and heads) because the public does not trust just a routine spokesman. They want confidence to be instilled by someone who is in a position of authority and whom they can trust. Is there any formal input, formal education, formal awareness program for dealing with the public on such issues in the event of a mishap?

Another participant replied that he didn't believe there is one, but strongly agreed that everyone finds themselves incomplete in these circumstances. It would be better placed to use all of our convictions and commitment, and in addition to have the background and experience and learning from others. This is very important. Would it be helpful to have an orientation of one or two days for leaders of various programs who would be called upon to communicate with the public?

Shri B. Bhattacharjee commented that the first responders will be the first on the scene in a nuclear event. There is a slight difference between nuclear event scenarios and natural event scenarios because in natural event scenarios, one can heavily rely on tradition and knowledge. Unless one relies on and captures their wisdom and knowledge base, responses in nuclear event scenarios will be a failure. With regard to a radiological emergency or disaster, there is another difference because that is where the advantage of Generation Program becomes all the more important. It may not be obvious to responders what to do in these events. The National Disaster Management Authority has no authority to make decisions on the ground (and other agencies do not have that role), therefore a specialist to the local administrator would be helpful. Elected officials may also have difficulties due to the need for reelection. People may have more confidence in elected officials whom they have elected. Information must be delivered in local languages by elected officials in the way they think is best

(e.g., hanging posters on boxes, or at railway stations, or via weekly or monthly gatherings).

In addition, India has a National Disaster Response Force with about 12,000 people, one of the largest in the world, with a dedicated force for disaster management including severe disasters. This force works with local forces and trains them as well. At a time of peace, prior to a disaster, these forces should prepare people at the grassroots level, accepting the help of the "home wards." This should be the model for responses to nuclear events. It is the single most important thing that should be done because if one wants to grow using public money, and if that growth occurs without public confidence, it will not work. No matter how great a genius one may be in this area, he or she must be allowed to speak without any question.

With regard to training people or courses for communicating complex issues to the public, another participant remarked that the many communication courses available to him and his colleagues focused on good communication skills in general, including how to make a limited number of points clearly, and not be too complex. A class specifically on how to communicate scientific uncertainties without causing panic would be helpful to develop. Other issues to address in such a class would be how to communicate topics unique to science and the realities of what experts deal with to the people.

9

General Discussion and Suggested Future Actions

General Discussion

The moderator began the final session by asking for feedback from all of the participants on what they felt about the workshop, and if there are points or comments to make for the next meeting.

Ambassador Ghosh noted that she was grateful that the organizers of the workshop included those who are not nuclear scientists, but who are interested in the subject. And she thought this interaction was very beneficial. One area that is worth considering is the issue of public awareness. Perhaps best practices in this area could be on the agenda at a future session, particularly how to address a very disparaged public. Many in India share a concern about nuclear power, hydroelectric power, or this or that, but they want power. This also happens in the United States, Ghosh said. Yes, they want nuclear power, but not in their backyard. So we need to have professional communicators because it is not fair to ask a nuclear scientist to go and speak to the church community, for example in Kudankulam, or to some other group. Given the diverse populations in India and the United States, communicating with them would be something to discuss in the future. Another suggestion would be to discuss Human Reliability Programs for personnel in more detail in the future.

Another participant from India recalled the joint statement between the leaders of India and the United States during President Barak Obama's visit in November 2010, where "They expressed a commitment to strengthen international cooperative activities that will reduce the risk of terrorists acquiring nuclear weapons or material." Participants in this workshop would be acting in accordance with this statement by trying to develop specific ideas or proposals to further the goal stated by the leaders. Cooperative, bilateral projects to strengthen best practices, norms, or standards would be helpful. Other, more ambitious possibilities, such as those in various forums such as the International

Atomic Energy Agency (IAEA) and the Global Initiative to Combat Nuclear Terrorism, should be encouraged. Undertaking joint publications on the topics discussed, such as the state of the art in nuclear forensics and attribution would also be worthwhile. In particular, one possibility which is a little ambitious, but which should be considered, the participant said, is the formation of a joint, publicly-announced team capable of offering services for detection and forensic investigation of an incidence of illicit trafficking to any country in the world that feels handicapped or feels the need for them. Such a joint team could be a measure of taking things forward and building a profile as two open societies, both with advanced nuclear capabilities.

NAS Summary

Rita Guenther thanked workshop participants, first and foremost, the distinguished presenters and guests for an excellent three days of exchange of views, and the very open and frank discussion.

She highlighted a few themes that emerged from the discussions, which, in her view, may serve as a foundation for joint cooperation. This list of themes is certainly not comprehensive; there are many more themes which have emerged, but the following can serve as a concrete foundation for going forward.

1. The need for better understanding of how to measure and characterize nuclear materials.
2. The opportunity to bring together collective knowledge of nuclear materials and methodologies to raise overall understanding, for example, through better and more effective databases.
3. The need to better understand, detect, and interrupt those who may represent a threat to nuclear security, be they insiders, be they terrorists, or a combination thereof.
4. The need to harness new, modern, and cutting-edge technologies and methodologies, to strengthen the broad spectrum of essential security infrastructures, including those related to cyber security.
5. The need and opportunity for continuous exchanges of best practices by learning from technical experts of our countries. This may take a variety of forms over the coming years, but may serve as a foundation and a basis to begin immediately.

Having listened to the last three days of discussions, Guenther commented that there is a very solid basis upon which we can build as our two countries take these discussions to the next phase of concrete cooperative joint efforts. At the close of this workshop, Guenther continued to be extremely optimistic about the prospects for addressing our common goal of nuclear security through the joint work of our technical experts.

Raymond Jeanloz also thanked the speakers for their incredible array of expertise, which allowed for a remarkable workshop. For example, Raj, an eminent scholar, director of a major laboratory, described one perspective from first-hand experience. In a very complimentary manner, Tharakan spoke from the law enforcement perspective of someone who has seen the realities on the ground. This is an amazing diversity of views, but absolutely essential to the topic at hand. This is not only a reflection of the cross-disciplinary nature of the workshop, but also of the excellence of the participants.

We started this workshop, he said, with a comment regarding the dangers that nuclear power faces, even though we all acknowledge that nuclear power will play an essential role in sustaining the immediate energy needs that the world faces. Nuclear power and nuclear materials present dangers whereby an incident anywhere around the world influences profoundly nuclear power everywhere around the world, and we have mentioned Fukushima, Three Mile Island, Chernobyl, but we can also imagine many other such instances.

Nuclear sabotage and terrorism are also key issues, whether an incident were to involve radiological dispersion or even the more extreme, and hopefully the much less likely the possibility of an improvised nuclear device. Again, an incident anywhere around the world would have huge ramifications in every capital around the world. Therefore, Jeanloz reinforced the message that we really are in this together, and we have to work together, first and foremost, to think about crisis response before an incident were to occur. What needs to be sorted out in the decision making process? What are the channels of communication? We need to benefit from the insights that each one of us can bring to these topics. Therefore international collaboration is essential and that is exactly why we are here, to initiate this collaboration.

Jeanloz proposed a path forward in two ways. First, a process by which we might move forward to undertake some of the concrete collaborative actions that Guenther alluded to, and second to illustrate possible areas of collaboration. These are purely for illustrative purposes because it is critical to have a means of iterating, improving, elaborating, and adding to some of these ideas. To move forward, Jeanloz suggested building on the existing channel of communication and cooperation between the National Institute for Advanced Studies (NIAS) and the National Academy of Sciences (NAS) to think through a handful of projects. The proposed projects should be useful and of mutual interest. As Raj stated, "They must be bold, but realistic."

As an initial starting point, Jeanloz proposed six areas of potential cooperation:

1. Detectors and sensors and sensor systems, detector systems, whether for NDA (nondestructive analysis) or for security or anything in between. There was interest in thermal infrared imaging sensors on the one hand, and the importance of sensor systems to the whole arena on the other.

2. Chronometry for age-dating, which would include, for example, protocols, standards, and standardization. How does one validate the methods and determine uncertainties and cross-validate between capabilities of different countries?
3. Detectors and analytical approaches with regard to search engines and databases. The IAEA encouraged the development of national databases, but in the end, our goal is some amount of coordination and collaboration. That may take a lot of time, many years, for a truly international, multilateral, full-blown collaborative enterprise, but in the meantime, we can develop very effective bilateral capabilities. This can come out of a workshop such as this one between Indian and U.S. experts.
4. Insider threat. Today there is a great deal of emphasis on terrorism, and there are opportunities to discuss systematic approaches to mitigating, addressing, or reducing the likelihood of insider threats or terrorists. Personnel Reliability Programs are one example of how probabilities and some risk analysis are not necessarily independent, and we have to consider how to avoid falling into a trap of calculating a cumulative probability in a such a simplistic way that it overlooks the possibility of those very, very small cumulative thefts that were alluded to earlier.
5. Cybersecurity. Issues of protocols and standards, among others, are very important in this area, and clearly we can benefit from expertise in India and in the United States because both of our countries have technical expertise in these areas and we acknowledge that these are rapidly developing areas of technology and, by implication, rapidly evolving threat areas potentially.
6. Training. For example, Indian scientists could come to U.S. facilities, perhaps the Department of Energy facilities, to participate in some of our training programs, and then provide critiques, and ideas of improvement and feedback. Perhaps this may lead to an opportunity for a counterpart visit of U.S. scientists to India to participate in training classes. How do we amplify and improve our training capabilities on both sides? This is a very broad topic, and extends to issues raised during this closing session:
   a. Public outreach and how to help train ourselves in the technical community to do more effective public outreach.
   b. Nuclear security crisis response, for example, how does one prepare ahead of time to be able to respond to such crises?
   c. Exchanges of students from the United States to India or of Indian students to the United States. Both academia and national or government laboratories offer rich possibilities for collaboration in these areas.

In summary, Jeanloz said, the areas for possible collaboration are: detectors, chronometry, search engines, approaches for dealing with insider threats in ter-

rorism, cybersecurity, and training. This is a very quick illustration and just the beginning of the discussion that will lead to real, active, hands-on, collaborative projects involving technical interactions.

NIAS Summary

B.V. Sreekatan, as a graduate of the Massachusetts Institute of Technology, began his summary comments by expressing his appreciation for the help that he and many Indian students received from the United States in many ways, both technological and academic, that allowed them to build-up science in India. One thing we learned was self-reliance; that India could do as well in the field of science. In the last 10 to 15 years, a lot of collaboration has occurred between NIAS and NAS, and a variety of conferences have been held here and also at Goa to discuss various aspects relating nuclear energy, the Comprehensive Test Ban Treaty, and other topics. This workshop, however, is very special and we should continue with the topics listed, without worrying about a 'divorce' due to differences of opinion about reactor designs. The focus should be on keeping civilians safe. Social scientists and others should be included because we face a demand for power in India, and the plan is to use thorium in the future. What is the future of nuclear power in the light of these terrible accidents that have taken place, like Fukushima, Chernobyl, and Three Mile Island?

Immediately after the Chernobyl accident, Andrei Sakharov said, "Plainly, mankind cannot renounce nuclear power, so we must find technical means to guarantee absolute safety and exclude the possibility of another accident. The solution I favor would be to build reactors underground deep enough so that in the worst-case accident would not discharge radioactive substances into the atmosphere." And Teller said, "My solution in regard to the containment of nuclear material in case of an accident is to place nuclear reactors 300 to 1000 feet underground. I think that the public misapprehension of the risk can be corrected only by such clear-cut measures as underground facility."

There may be other alternative sources of energy and nuclear energy may not be the only solution, but countries like India have no solution at the moment. Our nuclear power production is only at the level of 3 percent of our total energy supply, and we need to increase the energy supply at least by a factor of 2 or 3, and even with that, we are having serious problems. Therefore, we have to continue present nuclear reactor activities. In the long-term, however, alternatives must be pursued. There are estimates that state that by 2020 to 2050, the world will need something like 4,000 gigawatts of nuclear power. Of that, the United States wants to produce 1,000 gigawatts of nuclear power.

Over the three days of the workshop, we have had excellent discussions, and from the opening session, we have had the goal of proposing positive takeaways that will translate into a few areas of focused and well-planned research interaction among the scientists of the two countries. NIAS and NAS can essentially act as catalysts and facilitators.

Appendix A

Workshop Agenda

India-U.S. Cooperation on Global Security:
A Workshop on Technical Aspects of Civilian Nuclear Materials Security

U.S. National Academies of Science and
The National Institute of Advanced Studies

October 29-31, 2012
Indian Institute of Science Campus
Bangalore, India

GOALS AND OBJECTIVES OF THE WORKSHOP

This Indian-U.S. workshop on the technical aspects of civilian nuclear materials security has been convened jointly by the U.S. National Academy of Sciences (NAS) and the National Institute of Advanced Studies (NIAS) in Bangalore. The goals and objectives of this joint workshop are:

- To build mutual understanding of how experts in India and the United States approach issues of civilian nuclear materials management and security;
- To establish contacts among Indian and U.S. scientists and experts on nuclear materials security and to build confidence in cooperation on nuclear security issues, and;
- To identify concrete, technically-based areas for potential future collaboration between the technical experts of India and the United States, including through the Global Centre for Nuclear Energy Partnership.

Given these goals and objectives, NIAS and NAS encourage open and frank discussion during the workshop, and urge all participants to be actively engaged and seek specific opportunities for further collaborative scientific efforts.

DAY ONE – October 29, 2012

9:30 – 10:00	**Introductory Remarks**
	V. S. Ramamurthy, Director, NIAS
	Raymond Jeanloz, Professor, University of California Berkeley
Session I:	**Overview of Civilian Nuclear Materials Security: A Systems Approach** *Session Chair: V. S. Ramamurthy* *Rapporteur: Arun Vishwanathan*
10:05 – 10:25	M. R. Srinivasan, Former Chairman, Atomic Energy Commission
10:25 – 10:45	Robert Kuckuck, Former Director, Los Alamos National Laboratory (LANL)
10:45 – 11:30	Discussion
11:30 – 11:50	Coffee Break
Session II:	**Securing Nuclear Materials** *Session Chair: Raymond Jeanloz* *Rapporteur: Nabeel Mancheri*
	Overview of Nuclear Materials
11:50 – 12:10	R. Rajaraman, Emeritus Professor, Jawaharlal Nehru University
12:10 – 12:30	Ravi Grover, Director, Strategic Planning Group, Bhaba Atomic Research Centre (BARC)
12:30 – 12:50	Peter Santi, Scientist, Safeguards Science and Technology Group, LANL
12:50 – 13:30	Discussion
13:30 – 14:30	Lunch

Session III:	**Nuclear Forensics** *Session Chair: Ravi Grover* *Rapporteur: Sonika Gupta*
14:30 – 14:50	V. Venugopal, Dr. Raja Ramanna Fellow, Radio Chemistry and Isotope Group, BARC
14:50 – 15:10	Ian Hutcheon, Deputy Director, Glenn Seaborg Institute, LLNL
15:10 – 15:55	Discussion
15:55 – 16:15	Coffee Break
Session IV:	**Cybersecurity for Civilian Nuclear Materials Security** *Session Chair: Paul Singh, Oak Ridge National Laboratory*
16:15 – 16:35	Suresh Babu, Computer Division, BARC
16:35 – 16:55	Clifford Glantz, Senior Scientist, Pacific Northwest National Lab
16:55 – 17:40	Discussion
17:40	Adjourn
19:00	Dinner

DAY TWO – October 30, 2012

Session V:	**Technologies and Physical Security of Nuclear Materials** *Session Chair: Robert Kuckuck* *Rapporteur: Arvind Kumar*
9:30 – 9:50	Ranajit Kumar, BARC
9:50 – 10:10	M. Jordan Parks, Sandia National Laboratories
10:10 – 11:00	Discussion
11:00 – 11:20	Coffee Break

Session VI:	**Nuclear Security at Civilian Facilities** *Session Chair: V.S. Ramamurthy* *Rapporteur: Arun Vishwanathan*
	Reactor Facilities
11:25 – 11:45	Ranajit Kumar, BARC
11:45 – 12:05	Michael Browne, LANL
12:05 – 12:50	Discussion
12:50 – 13:50	Lunch
	Non-Reactor Facilities
13:50 – 14:10	A. R. Sundararajan, Former Head, Radiological Safety Division, Atomic Energy Regulatory Board (AERB)
14:10 – 14:30	Michael O'Brien, Associate Program Leader, Lawrence Livermore National Laboratory (LLNL)
	Safety, Security, Safeguards
14:30 – 14:50	Paul Nelson, Professor Emeritus, Texas A&M University
14:50 – 15:40	Discussion
15:40 – 16:00	Coffee Break
	Training on Nuclear Materials Security
16:00 – 16:20	Ranajit Kumar, BARC
16:20 – 16:40	Michael O'Brien, LLNL
16:40 – 17:20	Discussion

Special Lecture:	**Lowering Threats in Sustainable Development Using Nuclear Energy** *Chair: Arcot Ramachandran* *Rapporteur: K. P. Vijayalakshmi*
17:45-19:15	Anil Kakodkar, Former Chairman, Atomic Energy Commission
19:30	Dinner

DAY THREE – October 31, 2012

Session VII:	**The Human Factor in Nuclear Materials Security** *Session Chair: Stephen Cohen, Brookings Institution* *Rapporteur: Dr. M Mayilvaganan*
	Insider Threats
09:30 – 09:50	Hormis Tharakan, Former Director, Research and Analysis Wing
09:50 – 10:10	Philip Gibbs, Safeguards R&D Manager, Brookhaven National Laboratory
10:10 – 10:50	Discussion
10:50 – 11:10	Coffee Break
Session VIII:	**A Systems Approach to Civilian Nuclear Security: A Summary** *Session Chair: Raymond Jeanloz* *Rapporteur: M. Mayilvaganan*
11:10 – 11:30	Baldev Raj, Former Director, Indira Gandhi Centre for Atomic Research
11:30 – 11:50	D. V. Rao, Executive Advisor, LANL
11:50 – 12:30	Discussion

Session IX:	**General Discussion and Suggested Future Actions**
12:30 – 13:10	Session Chair Summaries
13:10 – 13:30	**Closing Remarks**
	Raymond Jeanloz B. V. Sreekantan, Visiting Professor, NIAS
13:30	**Adjourn and Lunch**

Appendix B

Statement of Task

SUMMARY

The National Academies, working with the National Institute of Advanced Studies (NIAS), will convene an Indian-U.S. workshop to identify and examine potential areas for scientific and technical cooperation between the United States and India on issues related to nuclear material security. The workshop may provide options for work that is of mutual interest for technical collaboration under the newly signed Memorandum of Understanding for the Global Centre for Nuclear Energy Partnership (GCNEP).

PROJECT CONTEXT AND OBJECTIVES

The U.S. government has made safeguarding of weapons-grade plutonium and highly enriched uranium an international policy priority, and convened The 2010 Nuclear Security Summit in Washington, D.C., on April 12 and 13, 2010. Forty-six governments sent delegations to the summit and twenty nine of them made national commitments to support nuclear security. During the Summit, India announced its commitment to establish a Global Centre for Nuclear Energy Partnership. The Centre is to be open to international participation through academic exchanges, training, and research and development efforts.

The Centre is "aimed at strengthening India's cooperation with the international community in the areas of advanced nuclear energy systems, nuclear security, radiological safety and radiation technology applications in areas such as health, food and industry".[1] In November 2010, the United States and India signed a memorandum of understanding that provides a general framework for cooperative activities in working with India's Centre. According to the White House, "In working with India's Centre, the United States intends to give priority to discus-

[1]Government of India. Ministry of Science and Technology. 13 August 2010. "Global Centre for Nuclear Energy Partnership." Available at: http://pib.nic.in/newsite/erelease.aspx?relid=64718. Accessed September 20, 2013.

sion of best practices on the security of nuclear material and facilities, development of international nuclear security training curricula and programs, conduct outreach with nuclear industry, and cooperation on other nuclear security activities as mutually determined".[2]

The Indian-U.S. workshop will identify and examine potential areas for substantive scientific and technical cooperation between the United States and India on issues related to nuclear material security. The parties involved hope that by doing so they will help to establish scientist-to-scientist contacts between experts in nuclear materials management in the United States and counterparts in India, build confidence in cooperation on nuclear security issues, and identify concrete, technically based areas for potential future collaboration, which could be the foundation for progress on the Centre.

The agenda for the workshop will be developed with Indian counterparts, but could include a variety of technical issues in nuclear materials management, such as nuclear materials safeguards, detection, monitoring, and nuclear forensics. The United States has active research programs on each of these topics, as well as related ones. The workshop will enable Indian experts to describe their work and plans for future activities. Because the workshop report will be a summary, the group will not prioritize the options discussed.

[2]U.S. Government. The White House Office of the Press Secretary. 8 November 2010. "Fact Sheet on U.S.-India Nuclear Security Partnership." Available at: http://www.whitehouse.gov/sites/default/files/india-factsheets/Fact_Sheet_on_Nuclear_Security.pdf. Accessed September 20, 2013.

Appendix C

Biographical Sketches of Workshop Speakers and Session Moderators

R. M. Suresh Babu received his M.A.in physics from Indian Institute of Technology, Bombay and joined the Bhabha Atomic Research Centre (BARC) in 1984. Since then he has been engaged in development of safety-critical software and control system software for nuclear power plants (NPPs). He was the chief designer of the first software-based reactor protection system used in an Indian NPP. He has also developed many real-time nuclear plant simulators for operator training and control system testing. He has participated in the preparation of regulatory guidance applicable to computer-based systems of Indian NPPs. His latest interest is in instrumentation and control security for NPPs.

Michael C. Browne is a technical staff member in the Safeguards Science and Technology Group at Los Alamos National Laboratory (LANL). He earned his Ph.D. in nuclear physics from North Carolina State University in 1999, and has focused on technical safeguards issues for the past 13 years. He has developed advanced safeguards instrumentation for attended and unattended applications, and holds patents related to this work. He has coordinated several safeguards efforts for the National Nuclear Security Agency (NNSA) in Japan, the Republic of Korea, Kazakhstan, and Ukraine. He has worked closely with the International Atomic Energy Agency (IAEA) to develop and implement high profile safeguards solutions and has been recognized by the U.S. Secretary of Energy for his efforts.

Stephen Philip Cohen has been Senior Fellow in Foreign Policy Studies at the Brookings Institution since 1998. In 2004, he was named as one of the five hundred most influential people in the field of foreign policy by the World Affairs Councils of America. Cohen was a faculty member at the University of Illinois from 1965 to 1998. From 1992 to 1993 he was Scholar-in-Residence at the Ford Foundation, New Delhi, and from 1985 to 1987, a member of the Policy Planning Staff of the U.S. Department of State, where he dealt with South Asia. He has

taught at Andhra University (India) and Keio University (Tokyo), Georgetown University, and now teaches in the South Asian program of Johns Hopkins School of Advanced International Studies. Cohen has served on numerous study groups examining Asia sponsored by the Asia Society, the Council on Foreign Relations, the Asia Foundation, and the National Bureau of Asian Research; he is currently a member of the National Academy of Sciences (NAS) Committee on International Security and Arms Control (CISAC) and a trustee of the Public Education Center. Cohen was the co-founder and chair of the workshop on Security, Technology and Arms Control for younger South Asian and Chinese strategists, held for the past ten years in Pakistan, India, Sri Lanka, and China, and was a founding member of the Research Committee of the South Asian strategic organization, the Regional Centre for Security Studies, Colombo. Cohen has written, co-authored, or edited ten books. Cohen received B.A. and M.A. degrees in political science from the University of Chicago, and a Ph.D. in political science from the University of Wisconsin. He has conducted research in China, Britain, India, Pakistan, the former Soviet Union, and Japan. He received grants from several major foundations and serves as a consultant to numerous government agencies.

Philip Gibbs has 29 years of project management and subject matter expert experience in nuclear safeguards with emphasis in material control and accountability (MC&A) for the U.S. Department of Energy's (DOE) domestic and international programs. Gibbs currently is working as a safeguards research and development manager at Brookhaven National Laboratory supporting the U.S. material protection control and accounting (MPC&A) program with a focus on insider analysis and mitigation. Prior to moving to international work, Gibbs served as the Local Area Network Material Accounting System (LANMAS) project manager managing the development and implementation of LANMAS, a standardized inventory and control system for nuclear components and inventories among DOE contractors. At the DOE Savannah River Site, he worked as a MC&A manager for accounting, technical support, procedures, and training. Prior to that time, Gibbs worked as a measurement control engineer in the area of mass measurements and process tank calibrations. Gibbs has a B.S. in Business from Miami University (1983) and M.S. in Logistics from Wright State University (1989).

Clifford Glantz is a project manager and senior staff scientist for Pacific Northwest National Laboratory (PNNL). His research focuses on cybersecurity risk management, critical infrastructure protection, and emergency preparedness and response. Glantz is the program manager for PNNL's cybersecurity efforts in support of the U.S. Nuclear Regulatory Commission (NRC) and he leads projects in support of DOE's *Cybersecurity for Energy Delivery Systems (CEDS)* program. His recent work has also been conducted for the Institute for Information Infrastructure Protection and the U.S. Department of Homeland Security (DHS). Glantz is the current national chair of the DOE Subcommittee on Con-

sequence Assessment and Protective Actions (SCAPA) and a member of several technical working groups.

Ravi B. Grover graduated in mechanical engineering from Delhi College of Engineering in 1970 and joined BARC Training School to study nuclear engineering. He worked as a nuclear engineer for 25 years and specialized in thermal hydraulics. Simultaneously, he obtained a Ph.D. from the Indian Institute of Science (IIS), Bangalore in 1982. Presently, he is working as a Principal Advisor at DAE and is a member of the Atomic Energy Commission (AEC). He is concurrently working as Director of the Homi Bhabha National Institute (HBNI), and is responsible for running the university. As Principal Adviser, he deals with issues related to nuclear power policy of India, including the evolution of the nuclear legislative framework, energy studies, and international collaborations. Grover was a member of the team of officials involved in negotiations that led to opening up of international civil nuclear cooperation. He is also chair of the Indian delegation to the International Thermonuclear Experimental Reactor Council. He served as a member of the expert group, constituted by the director general of the IAEA, to examine multilateral approaches to the nuclear fuel cycle.

Grover is a fellow of the Indian National Academy of Engineering and President of the Indian Society of Heat and Mass Transfer. His recent awards include the INS Award in 2006 for Nuclear Reactor Technology, including nuclear safety; the Dhirubhai Ambani Oration Award in 2008; the Distinguished Alumnus Award in 2009 from the Delhi College of Engineering Alumni Association; and Distinguished Alumnus Award in 2011 from the IIS and the IIS Alumni Association.

Ian Hutcheon is the deputy director of the Glenn Seaborg Institute and leader of the Chemical and Isotopic Signatures Group in the Chemical Sciences Division at Lawrence Livermore National Laboratory (LLNL). Hutcheon is also the scientific lead for nonproliferation nuclear forensics at LLNL. Prior to joining LLNL in 1994, Hutcheon was senior research associate in the Division of Geological Sciences, California Institute of Technology, Pasadena, California for 12 years. He spent two years as a post-doctoral fellow and six years as a senior research associate at the Enrico Fermi Institute at the University of Chicago. Hutcheon received a B.A. (physics) at Occidental College, Los Angeles in 1969, and a Ph.D. in physics from the University of California at Berkeley in 1975. Hutcheon has authored over 170 publications in peer-reviewed journals in the areas of secondary ion mass spectrometry, early solar system chronology, metabolic processes in microbial organisms and nuclear forensics and nonproliferation. Hutcheon is co-author of *Nuclear Forensic Analysis*, the only textbook on nuclear forensics. Hutcheon has supervised the graduate education of two M.S. and eight Ph.D. students and directed the activities of 18 postdoctoral researchers. He is a member of the American Geophysical Union and the Microbeam Analysis Society, and a Fellow of the Meteoritical Society.

Raymond Jeanloz is a professor of earth and planetary science and of astronomy at the University of California at Berkeley. He has done pioneering work in mineral physics, measurement of materials properties and simulation of deep-Earth processes using diamond-anvil and shock-wave experiments, elucidation of the core-mantle boundary as a chemically reactive zone, and study of the role of water in mantle processes and deep earthquake generation. His research and teaching have been recognized through a MacArthur Award, the American Geophysical Union's Macelwane Award, and Fellowship in the American Academy of Arts and Sciences and American Association for the Advancement of Science. He previously served as chair of the National Research Council's Board on Earth Sciences and Resources. He is currently the chair of NAS CISAC in the Policy and Global Affairs Division, and was elected as a member of NAS in 2004.

Anil Kakodkar became the director of BARC in 1996 and was the chairman of the Atomic Energy Commission (AEC) from 2000 to 2009. Currently he holds the DAE Homi Bhabha Chair at BARC. Kakodkar, undeterred by the restrictions imposed by the international community, succeeded in developing various systems for pressurized heavy water reactors, in building the Dhruva reactor starting from the conceptual stage, in rehabilitation of Madras Atomic Power Station Units 1 and 2, both of which at one stage appeared to be on the verge of being written off, in conceptualization and development of the advanced heavy water reactor that realizes next generation objectives in addition to the use of thorium. Kakodkar played a key role in nuclear tests in 1974 and 1998 at Pokhran. India also demonstrated nuclear submarine powerpack technology under Kakodkar's leadership. His leadership significantly boosted India's nuclear power program notwithstanding uranium supply constraints. As a result, India's nuclear generation capacity is set to reach 10,000 MWe with the completion of projects already underway. Under Kakodkar's leadership, India has earned a distinctive status as a country with advanced nuclear technology.

Notable also are his innovative contributions to human resource development. The establishment of the National Institute of Science Education and Research, the DAE-Mumbai University Centre for Basic Sciences, and the Homi Bhabha National Institute are expected to result in a fresh wave of new talent for the acceleration of India's multifaceted atomic energy program. Kakodkar is currently leading efforts to take the Indian Institutes of Technology and the National Institutes of Technology to a world class level, develop solar energy, enhance excellence in higher and technical education and catalyze science and technology (S&T) based development in Maharashtra.

Robert Kuckuck is retired from the University of California and is currently consulting and serving on advisory boards for the three national nuclear weapons research laboratories. He is a member of the Nuclear Weapons External Advisory Board for Sandia National Laboratories and the Nuclear Weapons Com-

plex Integration Committees for both LLNL and LANL. Immediately prior to his retirement, he served as the director of LANL in 2005 and 2006. Kuckuck held research and management positions at LLNL for more than 37 years, culminating in his serving as deputy director from 1994 to 2001. His research at LLNL was predominantly in atomic and nuclear experimentation studying underground nuclear explosions. His management roles included overseeing physics research for nuclear weapons development, leading LLNL's research program for scientific verification of international nuclear testing and arms control treaties and having responsibility for LLNL underground nuclear testing program. As deputy director, Kuckuck was responsible for all operations at LLNL. He left LLNL in 2001 to become the first principal deputy administrator of the newly created NNSA of DOE. In 2003, he received the Secretary of Energy's Gold Award, DOE's highest honor. Kuckuck's major areas of expertise include management of scientific and nuclear research and associated facilities, nuclear weapons development and testing, and international nuclear nonproliferation and arms control. He has broad experience in government, university, and public relations. Kuckuck received his Ph.D. in applied science from the University of California at Davis, and his M.S. degree in physics from the Ohio State University. He did his undergraduate work in physics at West Liberty State College in West Virginia.

Ranajit Kumar graduated from the University of Calcutta in Electronics and Tele-Communication Engineering in 1984. He attended the post graduate Training School of BARC in the 1984-1985 academic year (28th class). He has more than 27 years of experience in a wide range of nuclear security areas. Kumar has been involved in the requirement analysis, design, and development of physical protection systems for various DAE installations covering almost the entire nuclear fuel cycle. He has developed several computer based systems such as Personnel Access Control System, and the Perimeter Intrusion Detection System. He has also been actively involved in the regulatory aspects of security of nuclear installations and is a member of the Committee for Review of Security Aspects of Nuclear Facilities (CRSANF) of the Atomic Energy Regulatory Board (AERB).

He has organized a number of training courses on various aspects of physical protection and nuclear security with IAEA and served as faculty for many national and international training courses on nuclear security. He has also participated in the development and review of various nuclear security series documents, development of course curriculum and course material for various training courses on nuclear security for IAEA. He is a member in the Nuclear Security Guidance Committee (NSGC) and Interface Group of the IAEA. Kumar is presently heading the Physical Protection System Section of the Control Instrumentation Division at BARC.

Paul Nelson received the B.S. (engineering physics) from Auburn University, and the M.S. (Physics) and Ph.D. (Mathematics) from the University of New Mexico. His native technical field was the mathematical and computational aspects of neutron transport theory. He served for approximately 15 years as editor of the journal *Transport Theory and Statistical Physics.* He is Professor Emeritus of computer science, nuclear engineering and mathematics at Texas A&M University. He is a fellow of the American Nuclear Society (ANS), former chair of its Mathematics and Computation Division, and served as a member of the ANS Special Committee on Nuclear Nonproliferation until its recent promotion to status as a Technical Group. In his current semi-retirement he serves as associate director for international programs in the Nuclear Security Science and Policy Institute at Texas A&M University. In that capacity he has served as principal investigator for several projects funded by the U.S. government directed toward fostering a culture of nuclear security among Indian university students matriculating in a nuclear-related field of science or technology. He has had contact with DAE since first visiting BARC and Indira Gandhi Centre for Atomic Research (IGCAR), then the Reactor Research Centre in 1981. He is coauthor, with T. V. K. Woddi and William S. Charlton, of the 2009 monograph *India's Nuclear Fuel Cycle: Unraveling the Impact of the U.S.-India Nuclear Accord*, published by Morgan and Claypool.

Michel O'Brien is responsible for managing and providing technical support in the protection of nuclear and infrastructure assets deemed critical to U.S. national security. He currently holds the LLNL position of Associate Program Leader for the Global Security Directorate's International Nuclear Material Protection Program and has over 30 years of domestic and international experience in the fields of vulnerability assessment, including insider analysis, and physical protection. He has participated in vulnerability assessments, insider analyses, training, regulatory development, inspections, and security upgrades of sites in the U.S. and world-wide. He has served on Department of Army, Department of Navy, and DOE working groups for the formulation of physical protection policy guidance and regulations and has provided similar support under U.S. bilateral work between the European Commission, IAEA, the Russian Federation, and China. O'Brien also supports DOE's Global Critical Energy Infrastructure Protection Program activities in the international oil and electricity sectors. O'Brien holds a B.A. from the University of Maryland.

M. Jordan Parks is a member of the technical staff and a subject matter expert in physical security and modeling and simulation with the international nuclear security engineering department at Sandia National Laboratories (SNL). As colead of the STAGE modeling and simulation project, Parks has supported multiple vulnerability analyses for both international and domestic sites. He is also a member of the development team for the STAGE modeling and simulation toolkit, and is a member of the Product Steering Committee for the tool. From 2005 through 2010, Parks supported the National Infrastructure Simulation and

Analysis Center on numerous projects involving statistical models of behavioral phenomena in complex adaptive systems. He has extensive experience in modeling and simulation, statistics and statistical modeling, data analysis and preparation, and psychological/behavioral research methods. Parks has an M.A. in organizational psychology and evaluation from Claremont Graduate University and a B.A. in psychology and sociology from the University of New Mexico.

Baldev Raj has served DAE over a forty-two-year period, until 2011. As distinguished scientist and director of IGCAR in Kalpakkam, he galvanized a whole community of staff, scientists, and engineers to advance several challenging technologies, especially those related to the fast breeder test reactor (FBTR) and the prototype fast breeder reactor (PFBR). He has nurtured and grown excellent schools in nuclear materials and mechanics non-destructive evaluation (NDE), corrosion, welding, separation S&T and robotics and automation. Raj has pioneered application of NDE for basic research using acoustic and electromagnetic techniques in a variety of materials and components. He is also responsible for realizing societal applications of NDE in areas related to cultural heritage and medical diagnosis. He is currently president of the International Institute of Welding, president of the Indian National Academy of Engineering, and president-researcher at PSG Institutions, Coimbatore. Raj is a fellow of Indian National Science Academy (INSA), Indian Academy of Sciences, National Academy of Sciences, India, and Indian National Academy of Engineering, The Third World Academy of Sciences, German Academy of Sciences, International Nuclear Energy Academy and Academia NOT, International. He is an Honorary Fellow at the International Medical Sciences Academy. He was alternate chairman of Senior Advisory Group of Nuclear Energy, IAEA, a member and chairman of Apex Committee on Nuclear Energy Safety of Atomic Energy Regulatory Board and plenary speaker at the Nuclear and Science and Technology in Society Forum, Kyoto on various facets of nuclear reactors and fuel cycles.

Author of more than 850 publications in refereed journals and books, 60 books, including special journal volumes, contributions to encyclopedia and handbooks, as well as owner of 21 patents, he has been recognized with more than 100 awards, 350 honor, plenary, and keynote talks, and editorial positions and assignments in esteemed national and international fora in more than 30 countries. He has been conferred Distinguished Alumnus Award of IIS, Distinguished Materials Scientist Award of Materials Research Society of India, National Metallurgist Award of Ministry of Steel, Government of India, the Padma Shri Presidential Honor, the Indian Nuclear Society Life Time Achievement Award (2011), the Homi J. Bhabha Gold Medal Award from the Prime Minister of India during the 99th Indian Science Congress (2012), and the Nayudamma Memorial Award in 2012.

Above all he has interacted with thousands of scientists and mentored hundreds of children, students, scientists and technologists, and has inspired them to carry

out scientific and technical activities with a high degree of professionalism and, at the same time, follow exemplary ethical practices.

R. Rajaraman is emeritus professor of physics at the Jawaharlal Nehru University (JHU) and currently co-chair of the International Panel on Fissile Materials and vice president of INSA. He is also a member of the Science and Security Board of the *Bulletin of Atomic Scientists*, of the India-Pakistan Track II Ottawa dialogue, and the Asia Pacific Leadership Network. He completed his Ph.D. in 1963 under the supervision of Nobel Laureate, Hans Bethe at Cornell University, where he subsequently was on the faculty. He then moved to the University of Southern California and the Institute for Advanced Study at Princeton before returning permanently to India in 1969. He was first at Delhi University before moving as professor to IIS, Bangalore in 1976, and later in 1993 to JNU. Over these years he has also been a long-term visiting scientist at Harvard University, Massachusetts Institute of Technology, Stanford University, Princeton University, and the European Organization for Nuclear Research in Geneva.

His primary research work for nearly five decades has been on different areas of theoretical physics, including nuclear theory, particle physics, quantum field theory, statistical mechanics, solutions and quantum hall systems. In addition, he has also been working on nuclear policy issues, both military and civilian. He has done technical research on missile defense systems, nuclear weapons accidents, early warning, nuclear civil defense, minimal deterrence, fissile material production and stocks in Pakistan and India. He played an active role in the 3-year long public debate on the Indo-U.S. Nuclear Deal, through op-eds, seminars, and pedagogical tutorials to the diplomatic, defense, and scientific communities.

Arcot Ramachandran obtained his M.S. and Ph.D. degrees from Purdue University. Upon his return to India in 1950, he joined the Indian Institute of Science (IIS) as a faculty member in the newly established Department of Power Engineering. From 1954 to 1955, he was a research engineer in Babcock & Wilcox R&D Centre in Renfrew, Scotland. He was then a post-doctoral fellow at Columbia University and Purdue University from 1955 to 1956, when he participated in the summer session on Advances in Heat Transfer at Massachusetts Institute of Technology. When he returned to IIS in 1957, he became head of the mechanical engineering department and in 1965, he headed the department of industrial management. He established a school of research in heat and mass transfer as well as a number of post graduate programs in mechanical engineering.

He was elected chair of the Preparatory Committee of the United Nations Conference on Science and Technology in 1977. In October 1978, he was appointed Under Secretary General and Executive Director of the newly established United Nations Centre for Human Settlements. During his tenure, the United Nations approved his initiatives on the Observance of World Habitat Day, the 1987 International Year of Shelter for the Homeless, and the Global Strategy for Shelter

with a goal of providing adequate shelter for all. In 1990, he launched the Sustainable Cities program in 12 cities, and the. UN Habitat program rendered technical assistance to 108 countries. Ramachandran is the recipient of many national and international awards and the recipient of several honorary degrees from universities in the United States, Europe, and India.

Valangiman Subramaniam Ramamurthy is presently the director of the National Institute for Advanced Studies (NIAS). Ramamurthy is a well-known Indian nuclear scientist with a broad range of contributions from basic research to science administration. Ramamurthy started his career at BARC, Mumbai in 1963. He has made important research contributions, both experimental and theoretical, in many areas of nuclear fission and heavy ion reaction mechanisms, statistical and thermodynamic properties of nuclei, physics of atomic and molecular clusters and low energy accelerator applications. From 1995 to 2006, Ramamurthy was fully involved in the promotion of science promotion in India as Secretary to the Government of India, Department of S&T in New Delhi.

He was also the chairman of the IAEA Standing Advisory Group on Nuclear Applications for nearly a decade. After retirement from government service, Ramamurthy, in addition to continuing research in nuclear physics in the Inter-University Accelerator Centre in New Delhi, he has also been actively involved in human resource development in all aspects of nuclear research and applications. Ramamurthy is also a chair of the Recruitment and Assessment Board for the Council of Scientific and Industrial Research and a member of the National Security Advisory Board (NSAB). In recognition of his service to the growth of S&T in India, Ramamurthy was awarded one of the top civilian awards of the country, the Padma Bhushan Award, by the Government of India in 2005.

Dasari V. Rao is a nuclear engineer with 25 years of experience in safety and safeguards of nuclear reactor and fuel cycle facilities. His technical areas of expertise include computational fluid dynamics, neutron and radiation transport, and risk assessment of engineered and complex socio-technical systems. He has over 30 publications in these fields. As a principal investigator, Rao worked closely with the NRC and DOE in developing and implementing regulations governing emergency core cooling system reliability in commercial power reactors, protection of nuclear materials and facilities from terrorist threats, and designing-in inherent safety into advanced nuclear systems.

Following the Macondo disaster, he has been assisting DOE and the Department of Interior in assessing risk-reduction technologies for ultra-deepwater drilling in the Gulf of Mexico. Rao has held several leadership positions at LANL. Until recently (2004-2012), he was division leader of the Decision Applications Division. He also served as the program director of LANL's Defense and Homeland Security Office, which was responsible for overseeing all work performed at LANL in support of the Department of Defense and DHS. Presently, Rao is executive advisor to the associate director for threat identification and response. In

this new role, he is integrating LANL capabilities in the fields of advanced nuclear power systems and nuclear cybersecurity.

Peter Santi is a scientist in the Safeguards Science and Technology Group at LANL. He received his B.A. in physics from Marquette University in 1992. He went on to the University of Notre Dame where he earned his M.A. in 1996, and his Ph.D. in nuclear physics in 2000. Before coming to LANL as a postdoctoral research associate in 2003, he spent 3 years as a visiting research associate in nuclear astrophysics at the National Superconducting Cyclotron Laboratory at Michigan State University. Santi is an expert in developing and performing nondestructive assay (NDA) measurements of plutonium and uranium materials for both MC&A purposes as well as for international safeguards. Santi has taught various courses on NDA measurement techniques for both domestic customers and various international customers including at IAEA. At LANL, Santi is currently serving as both the Safeguards Technology Training Coordinator and the LANL Program of Technical Assistance to IAEA Safeguards Coordinator, responsible for managing the safeguards research and support projects that are being performed at LANL for IAEA.

Surinder Paul Singh, Ph.D., is a Senior Research and Development staff member at the Oak Ridge National Laboratory. He started his career developing remotely maintainable solvent extraction process equipment for nuclear fuel reprocessing facilities. He served as a project manager for technology development and the remediation of soils and groundwater contaminated with volatile organic compounds and radionuclides at the Rocky Flats Plant in Colorado. Since 1996, he has been involved in the development and implementation of technologies for nuclear security.

B. V. Sreekantan is currently a visiting professor at NIAS and also chair of the Gandhi Centre of Science and Human Values of the Bharatiya Vidya Bhavan in Bangalore. He was the director of the Tata Institute of Fundamental Research from 1975 to 1987, and the INSA Srinivasa Ramanujan Professor from 1987 to 1992. He has specialized in cosmic rays, high-energy physics, and high-energy astronomies and has published over 200 research papers. He has received a number of professional awards including the R.D. Birla Award of the Indian Physics Association, and the Padma Bhushan. He has held a number of visiting positions including in the United States and Japan.

After moving to NIAS, Sreekantan shifted his interests from pure science to philosophical studies on consciousness and exploration of commonalities and similarities in holistic approaches in modern science and ancient philosophies. Through two seminars he organized at NIAS, the historical epistemological, mathematical, experimental, and technological factors that laid the foundations of sciences and led to the growth of modern science over the last few decades

were analyzed and these have been incorporated in a volume currently being published by the Indian Council of Philosophical Research.

M. R. Srinivasan, is a member of AEC and has served as one of India's foremost nuclear energy experts and science bureaucrats. He was chair of the AEC and Founding Chair of the Nuclear Power Corporation of DAE from 1987 to 1990, having joined DAE in 1956 as an early member of Homi Bhabha's team, where he played a central role in the establishment of nuclear power stations. He served as advisor to the IAEA from 1990 to 1992, as a member of the Planning Commission from 1996 to 1998, and as a member of the NSAB from 2000 to 2008. He is a founding member of the World Association of Nuclear Operators. He has received the Padma Bhushan Award, the Padma Shri Award, the Indian National Academy of Engineering Lifetime Achievement Award, the Homi Bhabha Lifetime Achievement Award from the Indian Nuclear Society, the Homi Bhabha Gold Medal from Indian Science Congress, and the Sir M. Visvesvaraya Award for 2011 from the Government of Karnataka. He is the author of *From Fission to Fusion: The Story of the Indian Nuclear Power Programme* and "From the Desk of a Nuclear Scientist." He has written in *The Hindu* on nuclear issues and nuclear power related matters for many years.

A.R. Sundararajan, after graduating from 8th class of Training School at BARC in 1965, he started his career as a health physicist in fuel reprocessing and waste management plants in Trombay. Later he moved to Kalpakkam where, as head of the Health and Safety Division, he was responsible for organizing surveillance of radiation protection at IGCAR. He was instrumental in starting a strong research group on internal dosimetry, accident source term and aerosol research. He was associate director of Safety Research and Health Physics Group at IGCAR from 1997 to 1998. Later he moved to the AERB and was associated with more than 20 Safety Review Committees for various nuclear fuel cycle facilities. He was entrusted with the responsibility of setting up the Safety Research Institute (SRI) at Kalpakkam. He has to his credit 85 publications in the area of radiation protection. His areas of special interests include safety of fuel reprocessing, fast reactor safety and the environmental impact assessment of nuclear facilities. He has participated in several IAEA Technical Committee and Advisory Group meetings in the area of radiation protection, emergency preparedness and waste management. After his retirement in 2003 as director of the Radiological Safety Division of the AERB and director of SRI, he continues to serve on several committees of the AERB and the Ministry of Environment and Forest. Currently he is the chair of Safety Review Committee for the Application of Radiation in Industry, Medicine and Research of the AERB.

P. K. H. Tharakan, who belonged to the Kerala cadre of the Indian Police Service, retired in January 2007. He served the government in various capacities including Secretary in the Cabinet Secretariat of the Government of India and director general of Police in Kerala. After retirement, he served as advisor to the

Administrative Reforms Commission of India. He was also appointed by the President of India as advisor, to the Governor in 2007 and 2008, when the Presidential Rule was imposed in Karnataka. He served as a member of NSAB from 2008 to 2010. During that the same period, he was also chief advisor on Strategic Studies at BrahMos Aerospace, in addition to being on the board of directors of BrahMos Aerospace Trivandrum Limitea. Currently, he is an adjunct professor at the department of geopolitics and international relations at Manipal University and a distinguished scientist on the visiting faculty at IIS, Bangalore, researching security-related issues. Recently, he has been made a member of the State Security Commission of the Government of Kerala. He was also a member of the Committee on Prevention of Corruption, which submitted its report to the Chief Minister of Kerala in July, 2012. He is vice chair of the recently established Community Mediation Service Committee. He writes on issues related to geopolitics, terrorism, peace, and conflict resolution.

V. Venugopal, M.Sc., Ph.D, is presently a Raja Ramanna Fellow and retired as the director of the Radio Chemistry and Isotope Group at BARC. He is a specialist in the field of thermal/thermodynamics of plutonium based fuels at high temperature, chemical quality control of fuel, X-ray and solid state chemistry, and oversees radioisotope and radiation technology programs at BARC. From 2007 to 2011, he served as a member on the Standing Advisory Group for Safeguards to advice the director general on safeguard issues. He has to his credit more than 370 publications, of which 190 are published in reputed international journals. Widely acclaimed as an expert in the area of thermodynamics, he is the vice president of Indian Nuclear Society (INS). He is also a member of several professional bodies. He has received many awards including the Netzsch-Indian Thermal Analysis Society award in 2001, the International Symposium on Circuits and Systems silver medal in 2002, and the Materials Research Society of IndiaI medal for 2003-2004, the INS award for 2005, and the DAE award in 2007.

He was on deputation on Indo-German collaboration and worked at the Nuclear Research Centre in Julich, Germany for a year and a half and attended several conferences abroad to give lectures in the field of thermodynamics of nuclear materials. He led delegations to South Korea and Argentina for bilateral meetings on cooperation in the area of nuclear S&T. As an advisor for Ph.D. students at Mumbai University, 25 students have thus far obtained graduate degrees under his guidance.

Appendix D

Biographical Sketches of NAS Planning Committee Members

Raymond Jeanloz—University of California, Berkeley (Chair)

Raymond Jeanloz is a Professor of Earth and Planetary Science and of Astronomy at the University of California at Berkeley. He has done pioneering work in mineral physics, measurement of materials properties and simulation of deep-Earth processes using diamond-anvil and shock-wave experiments, elucidation of the core-mantle boundary as a chemically reactive zone, and study of the role of water in mantle processes and deep earthquake generation. His research and teaching have been recognized through a MacArthur Award, the American Geophysical Union's Macelwane Award, and Fellowship in the American Academy of Arts and Sciences and American Association for the Advancement of Science. He previously served as chair of the National Research Council's Board on Earth Sciences and Resources. He is currently the chair of the National Academy of Sciences' (NAS) Committee on International Security and Arms Control in the Policy and Global Affairs Division, and was elected as a member of the NAS in 2004.

Stephen P. Cohen—The Brookings Institution

Stephen Philip Cohen has been Senior Fellow in Foreign Policy Studies at the Brookings Institution since 1998. In 2004 he was named as one of the five hundred most influential people in the field of foreign policy by the World Affairs Councils of America. Professor Cohen was a faculty member at the University of Illinois from 1965 to 1998. From 1992-93 he was Scholar-in-Residence at the Ford Foundation, New Delhi, and from 1985-1987, a member of the Policy Planning Staff of the U.S. Department of State, where he dealt with South Asia. He has taught at Andhra University (India) and Keio University (Tokyo), Georgetown University, and now teaches in the South Asian program of Johns Hopkins School of Advanced International Studies.

Dr. Cohen has served on numerous study groups examining Asia sponsored by the Asia Society, the Council on Foreign Relations, the Asia Foundation, and the National Bureau of Asian Research; he is currently a member of the National Academy of Sciences Committee on International Security and Arms Control and a trustee of the Public Education Center. Dr. Cohen was the co-founder and chair of the workshop on Security, Technology and Arms Control for younger South Asian and Chinese strategists, held for the past ten years in Pakistan, India, Sri Lanka and China, and was a founding member of the Research Committee of the South Asian strategic organization, the Regional Centre for Security Studies, Colombo. Dr. Cohen has written, co-authored, or edited ten books. Professor Cohen received B.A. and M.A. degrees in Political Science from the University of Chicago, and a Ph.D. in Political Science from the University of Wisconsin, He has conducted research in China, Britain, India, Pakistan, the former Soviet Union, and Japan. He received grants from several major foundations and serves as a consultant to numerous government agencies.

Cherry Murray—Harvard University

Cherry A. Murray is Dean of Harvard University's School of Engineering and Applied Sciences; John A. and Elizabeth S. Armstrong Professor of Engineering and Applied Sciences; and Professor of Physics. Previously, Murray served as principal associate director for science and technology at Lawrence Livermore National Laboratory and was president of the American Physical Society. Before joining Lawrence Livermore in 2004, Murray was Senior Vice President of Physical Sciences and Wireless Research and had a long and distinguished career at Bell Laboratories Research. Murray was elected to the National Academy of Sciences in 1999, to the American Academy of Arts and Sciences in 2001, and to the National Academy of Engineering in 2002. She has served on more than 80 national and international scientific advisory committees, governing boards and National Research Council panels and as a member of the National Commission on the British Petroleum Deepwater Horizon Oil Spill and Offshore Drilling. She is currently chair of the National Research Council Division of Engineering and Physical Science. As an experimentalist, Murray is known for her scientific accomplishments in condensed matter and surface physics. She received her B.S. in 1973 and her Ph.D. in physics in 1978 from the Massachusetts Institute of Technology. She has published more than 70 papers in peer-reviewed journals and holds two patents in near-field optical data storage and optical display technology.

William H. Press—University of Texas, Austin

William H. Press is a computer scientist and computational biologist with broad interests in the physical and biological sciences. An experienced manager in both university and national laboratory settings, he is widely recognized for his academic and research accomplishments. Press holds the Warren J. and Viola M. Raymer Chair in Computer Sciences and Integrative Biology at the Universi-

ty of Texas at Austin (UT). At UT, his affiliations include membership in the Institute for Computational Engineering and Sciences and in the Institute for Cellular and Molecular Biology. Press is also a Senior Fellow (on leave) at the Los Alamos National Laboratory. In his research career, Press has published more than 150 papers in areas of computational biology, theoretical astrophysics, cosmology, and computational algorithms. He is senior author of the Numerical Recipes textbooks on scientific computing, with more than 350,000 hardcover copies in print. His current research is in bioinformatics and whole-genome genetics. At the time of his arrival at Harvard in 1976, Press was its youngest tenured professor. Earlier, he was Assistant Professor of Physics at Princeton University, and Richard Chace Tolman Research Fellow in Theoretical Physics at Caltech, where he received his Ph.D. in physics in 1972. His undergraduate degree was from Harvard in 1969. Elected to the NAS in 1994, he in 2000 became a founding member of NAS's new Computer and Information Sciences section.

Appendix E

List of Collaboration Topics Suggested by Workshop Participants

Overview

Following the joint India-U.S. workshop on technical aspects of civilian nuclear materials security, the workshop organizers from the National Academy of Sciences (NAS) and the National Institute for Advanced Studies (NIAS) received from the participants the following suggestions of potential topics and mechanisms for enhanced collaboration between scientists from India and the United States.

This is an initial list of topics generated during the workshop; subsequent topics may follow. The order in which these topics are listed does not in any way imply a prioritization. There are obvious topical overlaps, and overlaps in approaches, which can be further clarified.

This list is based on the technical opportunities identified by the participants, and does not necessarily reflect the desires and priorities of either government.

A. Personnel Reliability and Insider Threats

A1. Training: Human Reliability Program
A2. Training: Training Management
A3. Insider-Insider Protection Program
A4. Insider/Cyber-Insider Vulnerability Analysis
A5. Physical Protection-Performance Assurance Program
A6. Physical-Cybersecurity Integration

B. Cybersecurity

B1. Cybersecurity guidance for security controls at nuclear power plant facilities

B2. Cybersecurity guidance for security controls at other types of nuclear facilities
B3. Cybersecurity guidance for equipment acquisition
B4. Guidance for cybersecurity self-assessments
B5. Guidance for administrating and monitoring the performance of firewalls and intrusion detection/protection systems
B6. Investigate tools, technologies, and approaches for electronic testing of control systems for potential cyber vulnerabilities
B7. Guidance for deploying and maintaining defensive architectures
B8. Sharing/Exporting cybersecurity technologies
B9. Sharing threat and vulnerability information
B10. Guidance on cybersecurity inspection procedures
B11. Guidance on separation of duties for key information system insiders
B12. Guidance on how to integrate physical and cybersecurity programs

C. Nuclear Forensics

C1. Detection of uranium and plutonium in environmental matrices
C2. Age-dating of uranium-rich materials
C3. Round robin sample exchange
C4. National nuclear forensic libraries

D. Modeling and Simulations (Vulnerability Assessments)

D1. Methodology Tool Types: applications, strengths and weaknesses
D2. Training
D3. A path forward for possible joint cooperation

E. Physical Security

E1. Guard Forces: Composition, Training, Testing, Rotation, etc.
E2. Technologies for Physical Protection
E3. Integration of Technologies and Methodologies to Physical Protection
E4. Physical Protection as part of a systems approach to facility security (including personnel reliability programs, vulnerability assessments, etc.)

F. Material Measurements and Characterizations

F1. Material measurements and characterizations
F2. How they fit into materials characterization and accounting methodologies

G. Safety, Security, Safeguards

G1. Develop technology-neutral methods for estimating the frequency of attack for security
G2. Harmonize metrics for consequences between nuclear security and nuclear safety/safeguards
G3. Develop secure information technologies that would permit communication resources at a nuclear installation to be jointly used for safeguards and security

POSSIBLE MECHANISMS FOR FURTHER COOPERATION

- Training courses, either joint, reciprocal, phased, integrated, etc.
- Visiting scholars programs for students and/or young professionals at universities or laboratories
- Longer-term technical exchanges of experts to laboratories for joint work
- Workshops, either facilitated by the laboratories, NAS-NIAS, or other appropriate groups
- Site visits for specific scientific/technical purposes with well-defined objectives